WHAT REALLY IS pWCET?

A RIGOROUS AXIOMATIC PROPOSAL

RTSS 2023

6 December 2023

Sergey Bozhko, Filip Marković, Georg von der Brüggen, and Björn Brandenburg

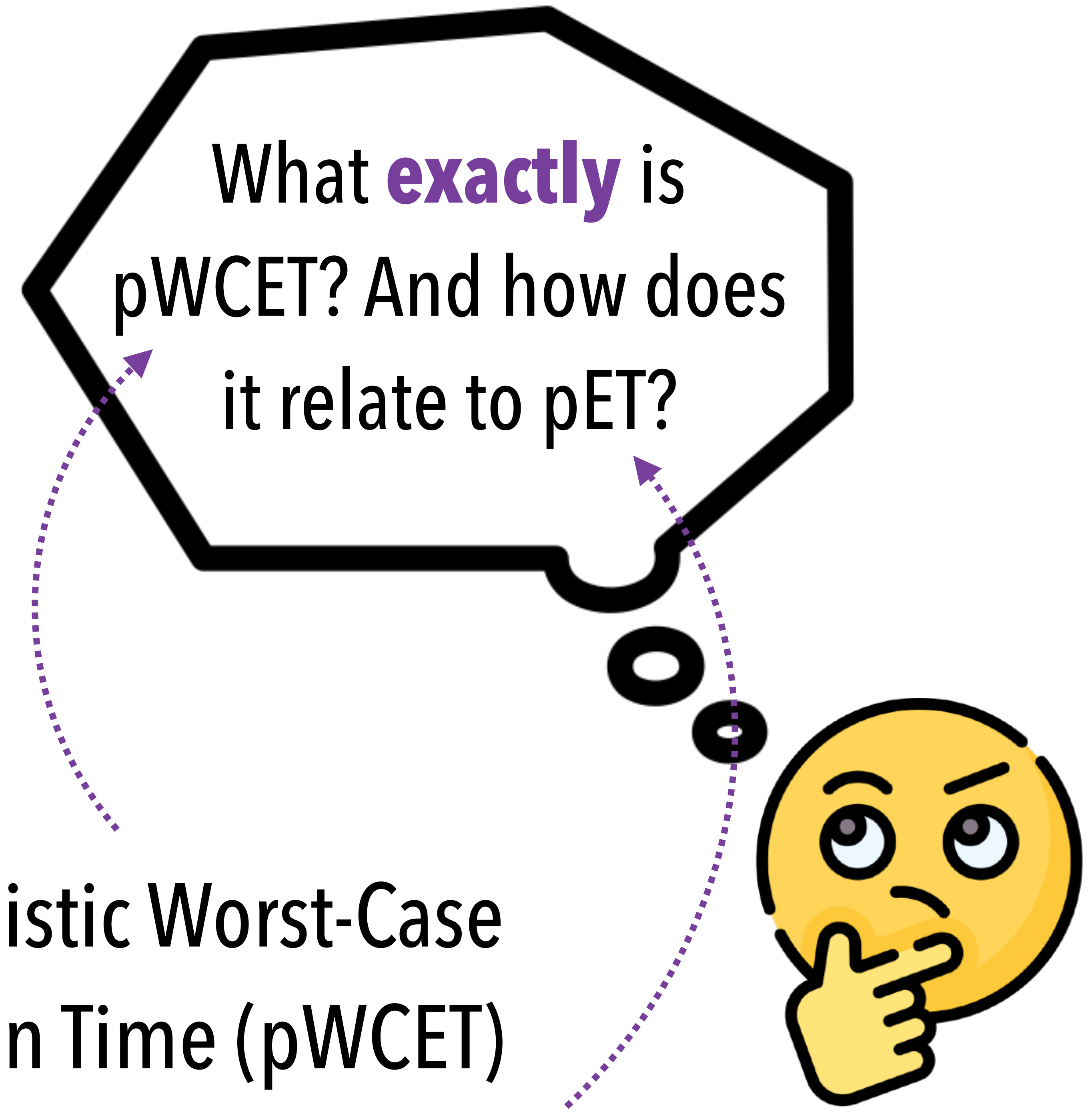
MAX PLANCK INSTITUTE FOR SOFTWARE SYSTEMS

technische universität dortmund

European Research Council
Established by the European Commission

MAX-PLANCK-GESELLSCHAFT

THIS PAPER IN A NUTSHELL



Probabilistic Worst-Case Execution Time (pWCET)

Probabilistic Execution Time (pET)

THIS PAPER IN A NUTSHELL

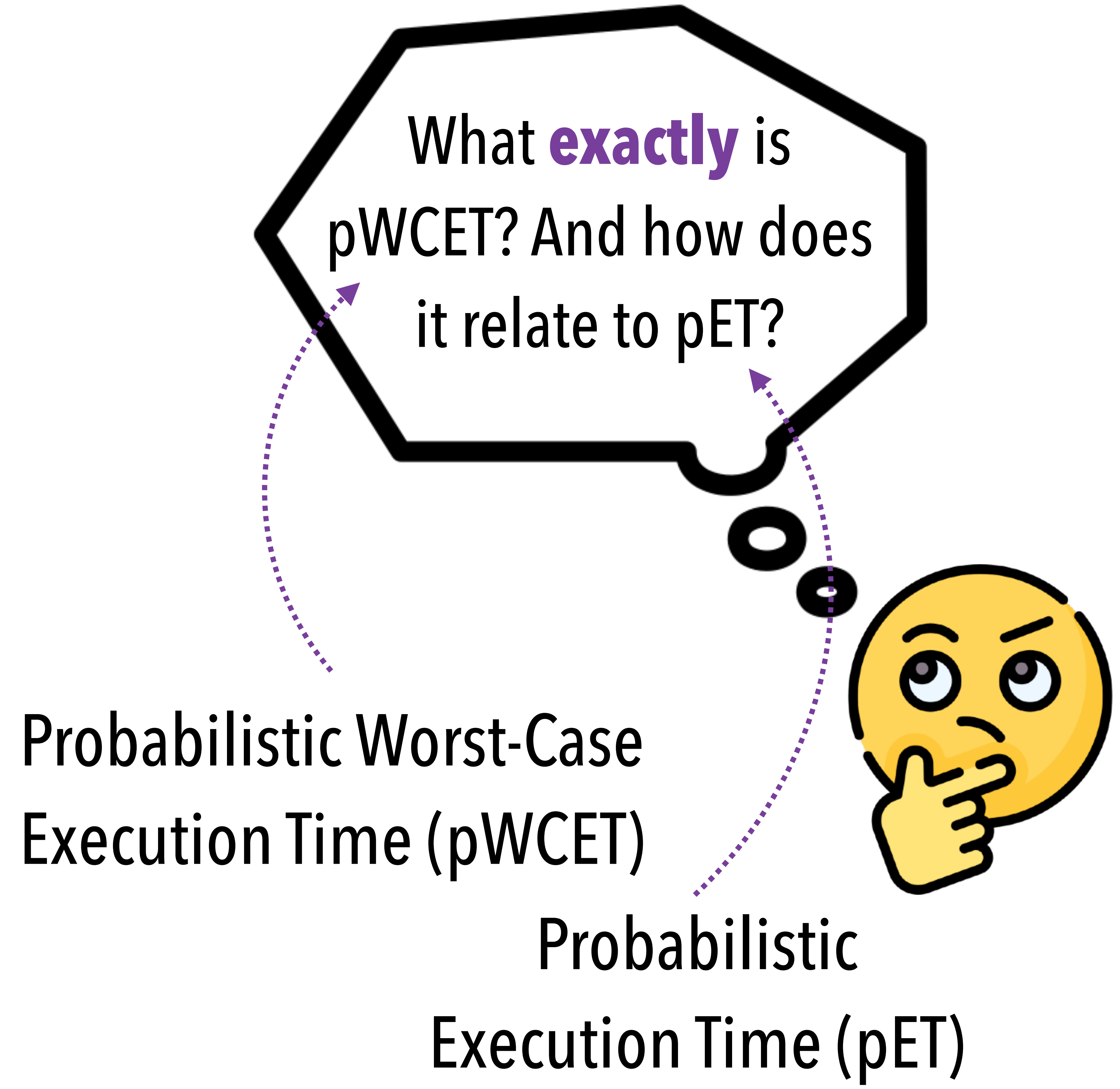
Independent and identically distributed

We propose

➔ First **fully formal** definitions of pET and pWCET

➔ **Adequacy property** capturing the notion of "IID upper bound on pET"

➔ **Prove** that our proposal of pWCET is adequate in this sense



THIS PAPER IN A NUTSHELL

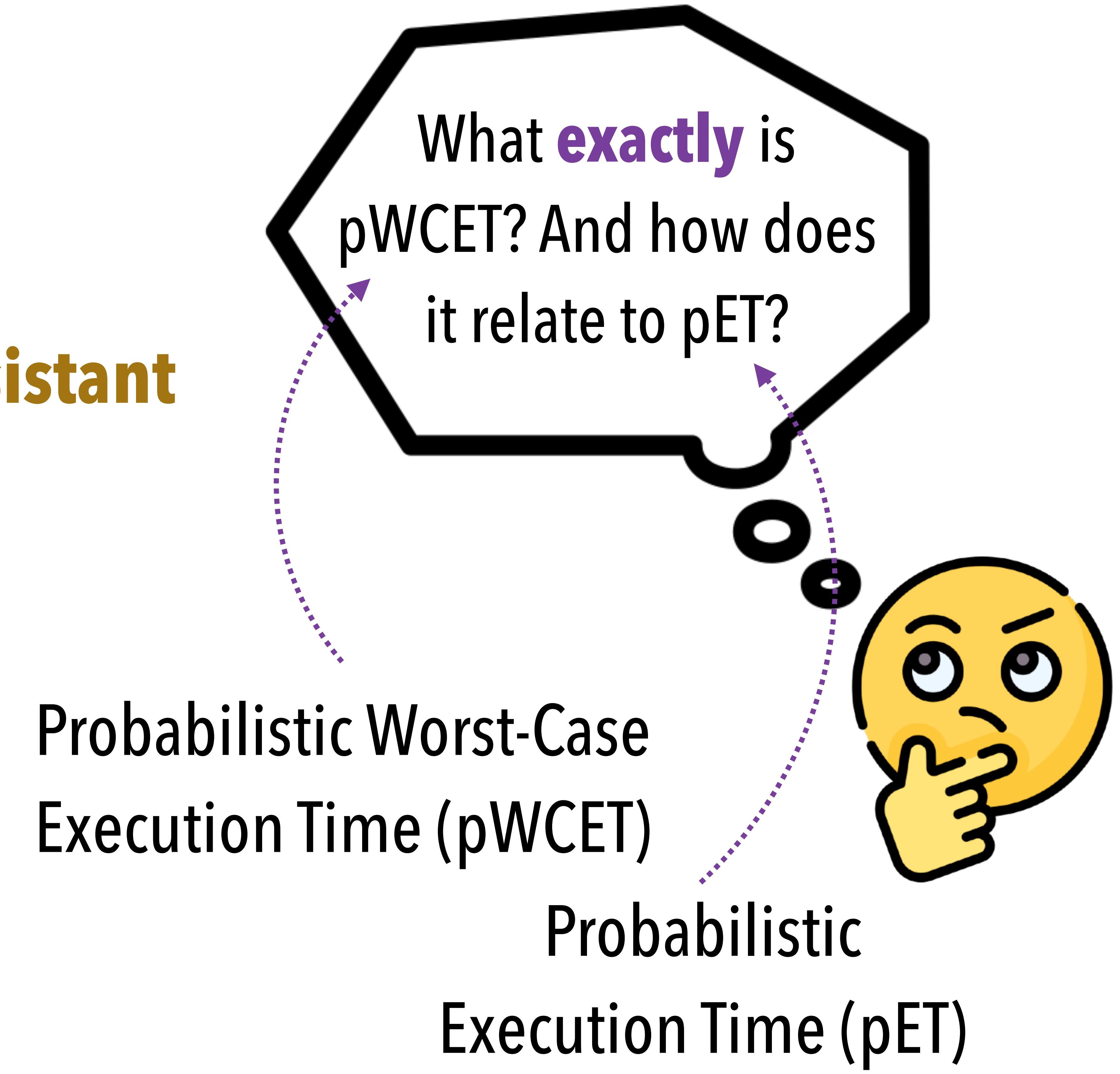
Independent and identically distributed

We propose

➔ First **fully formal** definitions of pET and pWCET

➔ **Adequacy property** capturing the notion of "IID upper bound on pET"

➔ **Prove** that our proposal of pWCET is adequate in this sense



We formalized our proposal with the Coq proof assistant

➔ Semantics of stochastic real-time systems

➔ Definitions of pET, pWCET, and the adequacy property

➔ **Machine-checked** proof that pWCET is adequate

The Coq Proof Assistant

coq.inria.fr

ANALYSIS OF REAL-TIME SYSTEMS: THE BIG PICTURE

THE BIG PICTURE

Predictions

THE BIG PICTURE

Worst-Case Execution Time (WCET)

To get the predictions right, we need:

- ➔ Model with the right **specification**
  - ➔ *E.g.*, model must include WCETs to allow (classical) response-time analysis

Model of the system

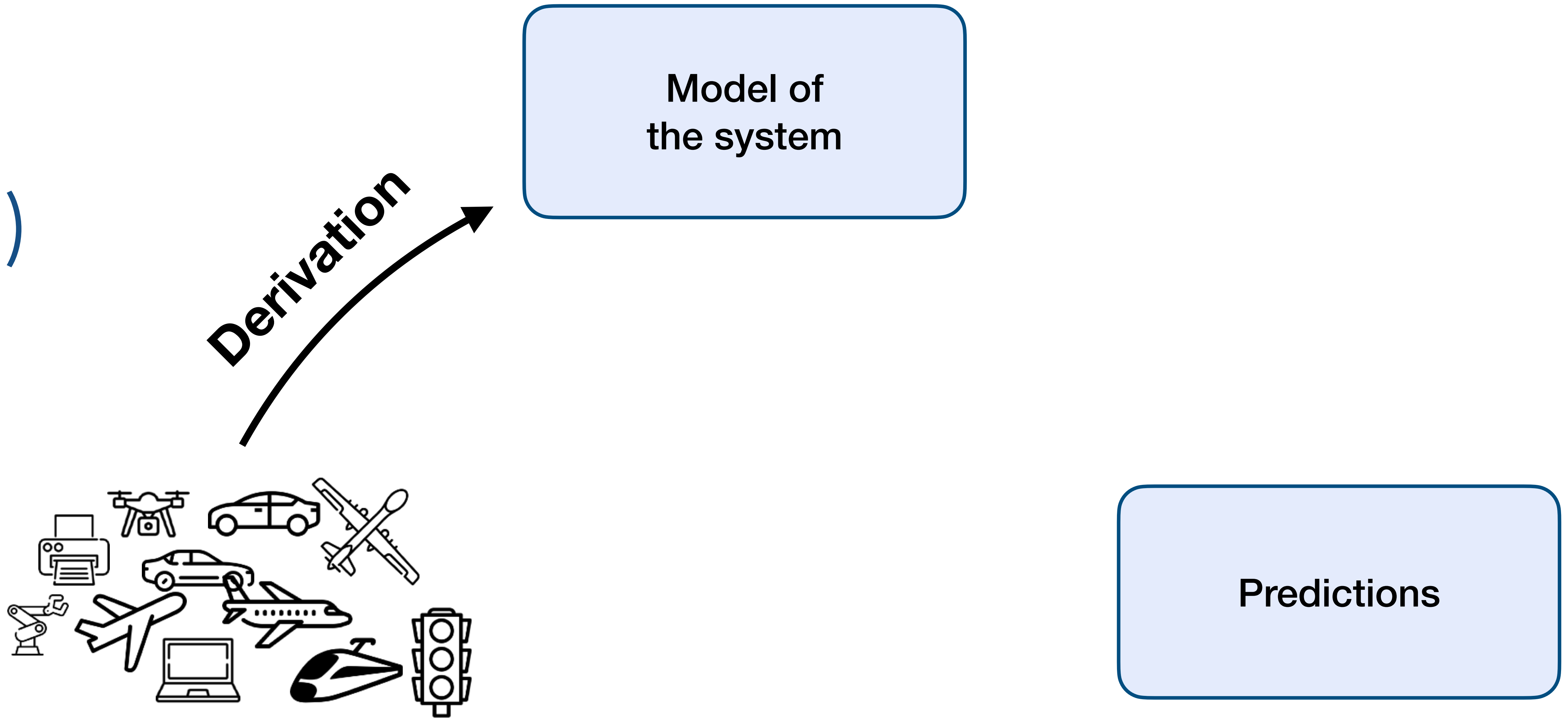
Predictions

THE BIG PICTURE

Worst-Case Execution Time (WCET)

To get the predictions right, we need:

- ➔ Model with the right **specification**
  - ➔ *E.g.*, model must include WCETs to allow (classical) response-time analysis
- ➔ Correct model **derivation**
  - ➔ Optimistic WCET bound $\Longrightarrow$ Wrong predictions

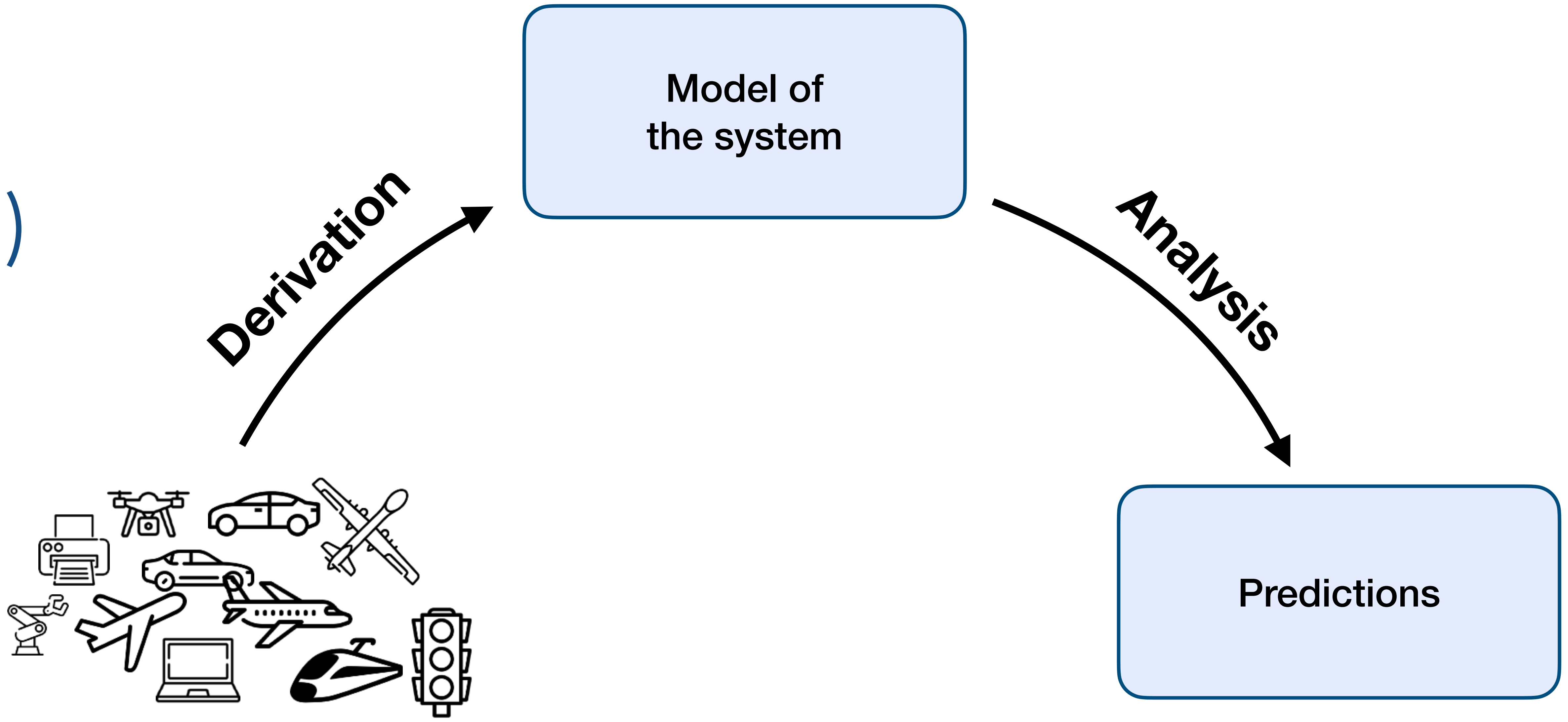


THE BIG PICTURE

Worst-Case Execution Time (WCET)

To get the predictions right, we need:

- ➔ Model with the right **specification**
  - ➔ *E.g.*, model must include WCETs to allow (classical) response-time analysis
- ➔ Correct model **derivation**
  - ➔ Optimistic WCET bound $\Longrightarrow$ Wrong predictions
- ➔ Correct **analysis**
  - ➔ Flawed analysis $\Longrightarrow$ Wrong predictions

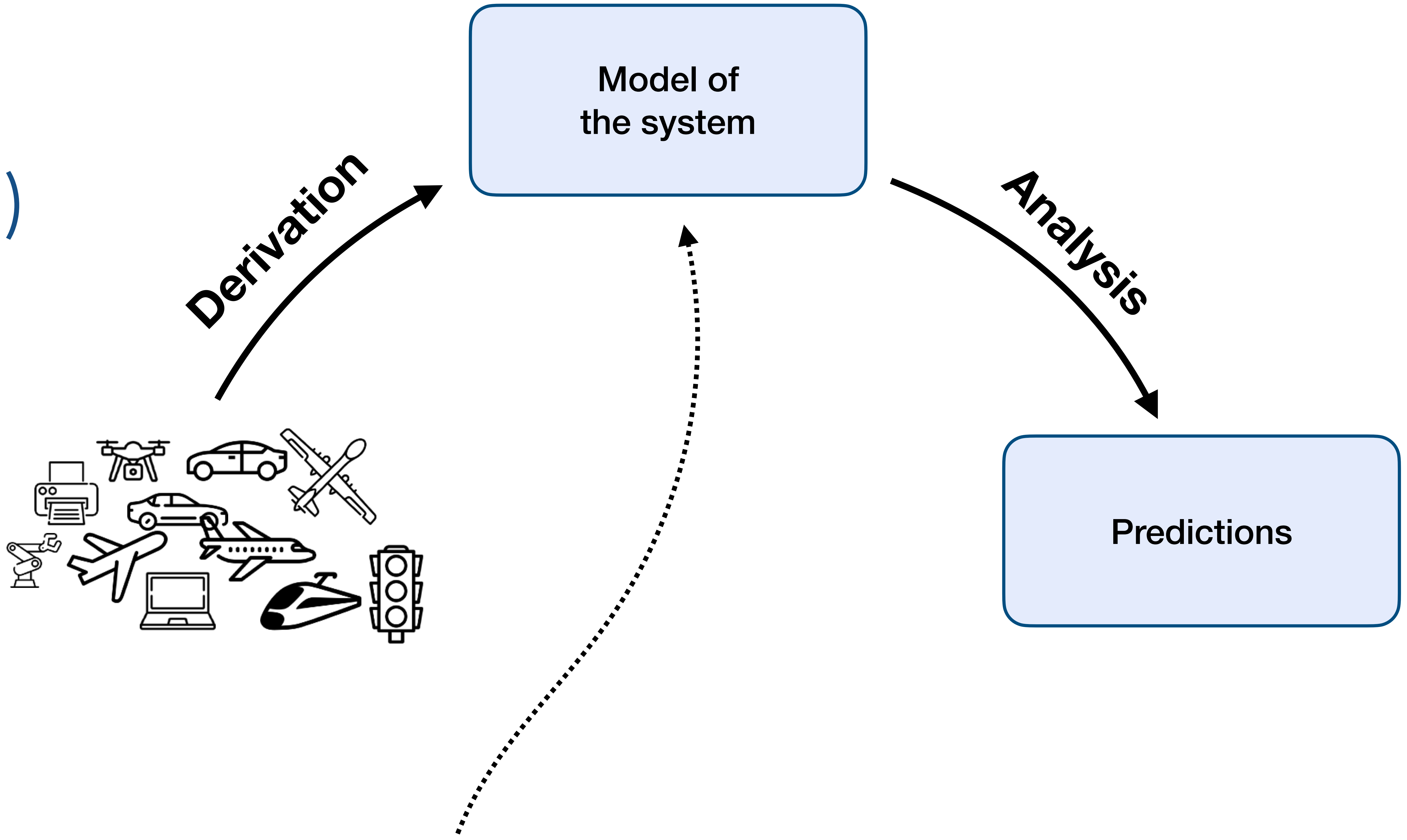


THE BIG PICTURE

Worst-Case Execution Time (WCET)

To get the predictions right, we need:

- ➔ Model with the right **specification**
  - ➔ *E.g.*, model must include WCETs to allow (classical) response-time analysis
- ➔ Correct model **derivation**
  - ➔ Optimistic WCET bound $\Longrightarrow$ Wrong predictions
- ➔ Correct **analysis**
  - ➔ Flawed analysis $\Longrightarrow$ Wrong predictions

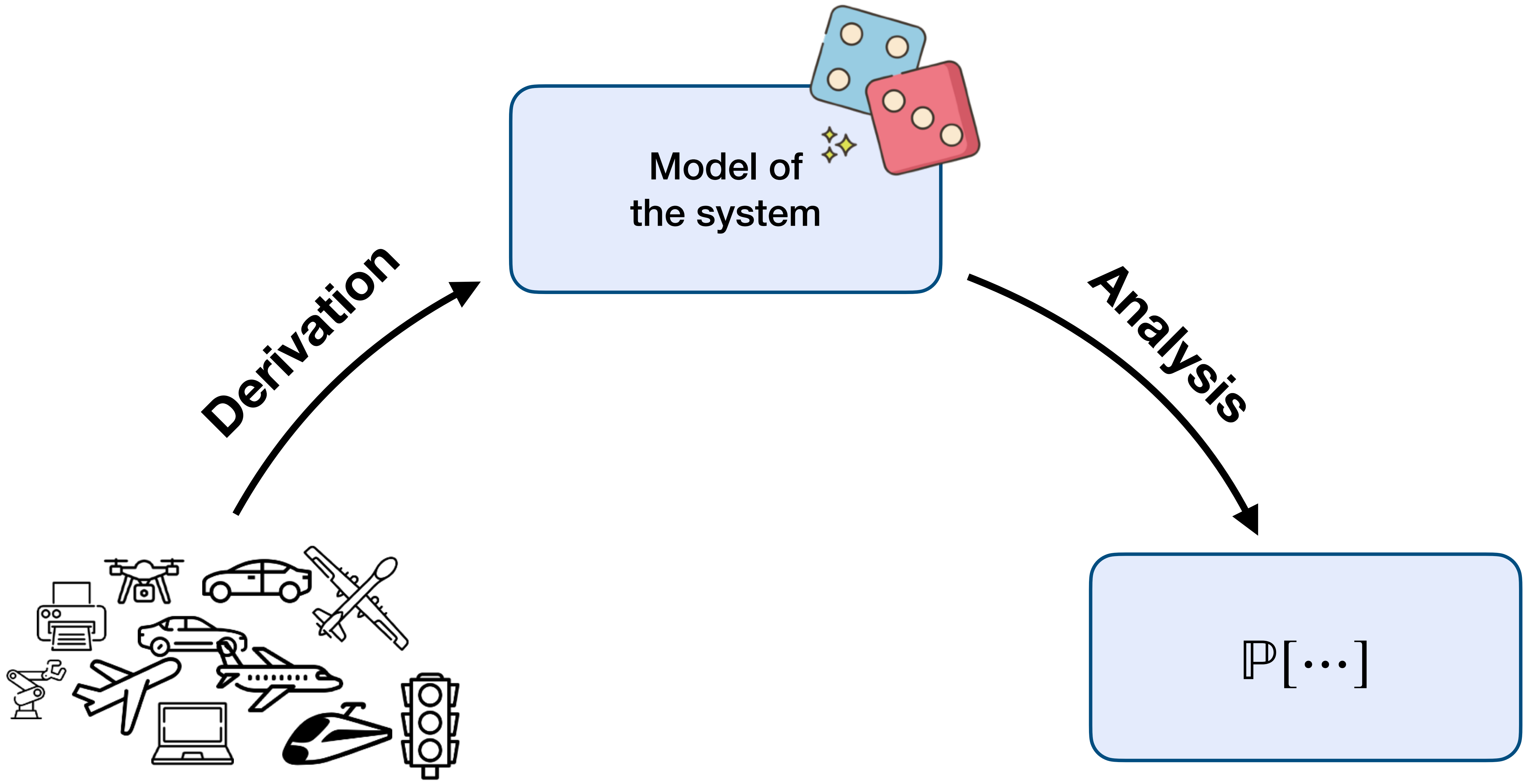


Interpretation of common models is pretty straightforward in the deterministic case

SPECIFICATIONS ARE LESS OBVIOUS IN THE STOCHASTIC CASE

To get the predictions right, we need:

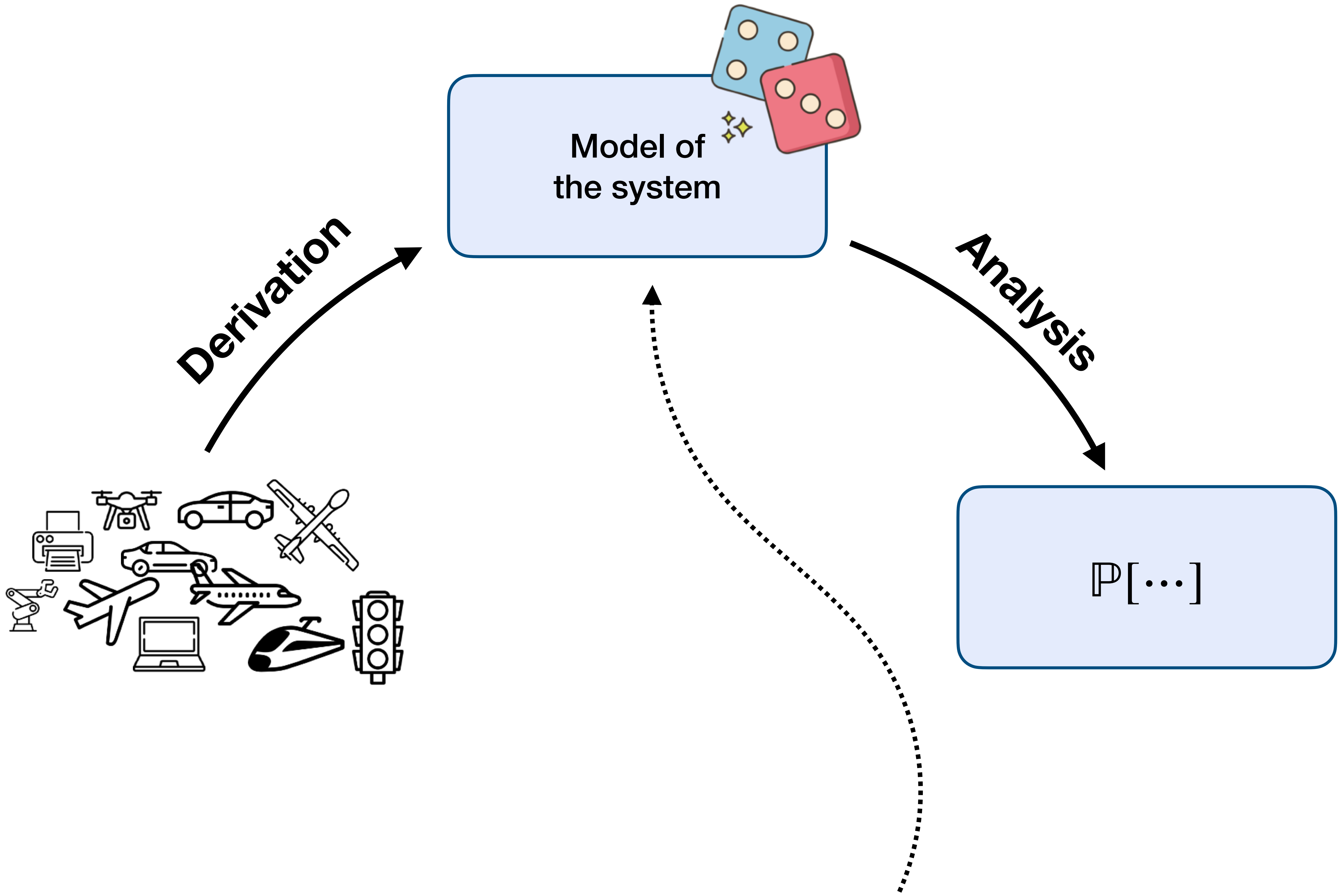
- ➔ Model with the right **specification**
  - ➔ *E.g.*, model must include ~~WCETs~~ **???** to allow (~~classical~~ probabilistic) response-time analysis
- ➔ Correct model **derivation**
  - ➔ Optimistic WCET bound $\Longrightarrow$ Wrong predictions
- ➔ Correct **analysis**
  - ➔ Flawed analysis $\Longrightarrow$ Wrong predictions



SPECIFICATIONS ARE LESS OBVIOUS IN THE STOCHASTIC CASE

To get the predictions right, we need:

- Model with the right **specification**
  - *E.g.*, model must include ~~WCETs~~ **???** to allow (~~classical~~ probabilistic) response-time analysis
- Correct model **derivation**
  - Optimistic WCET bound $\Longrightarrow$ Wrong predictions
- Correct **analysis**
  - Flawed analysis $\Longrightarrow$ Wrong predictions



Specifications of stochastic RTSs are much less straightforward

THE CASE FOR STOCHASTIC RTS

Stochastic real-time systems

➔ Model of RTSs, where workload parameters are modelled *stochastically*

THE CASE FOR STOCHASTIC RTS

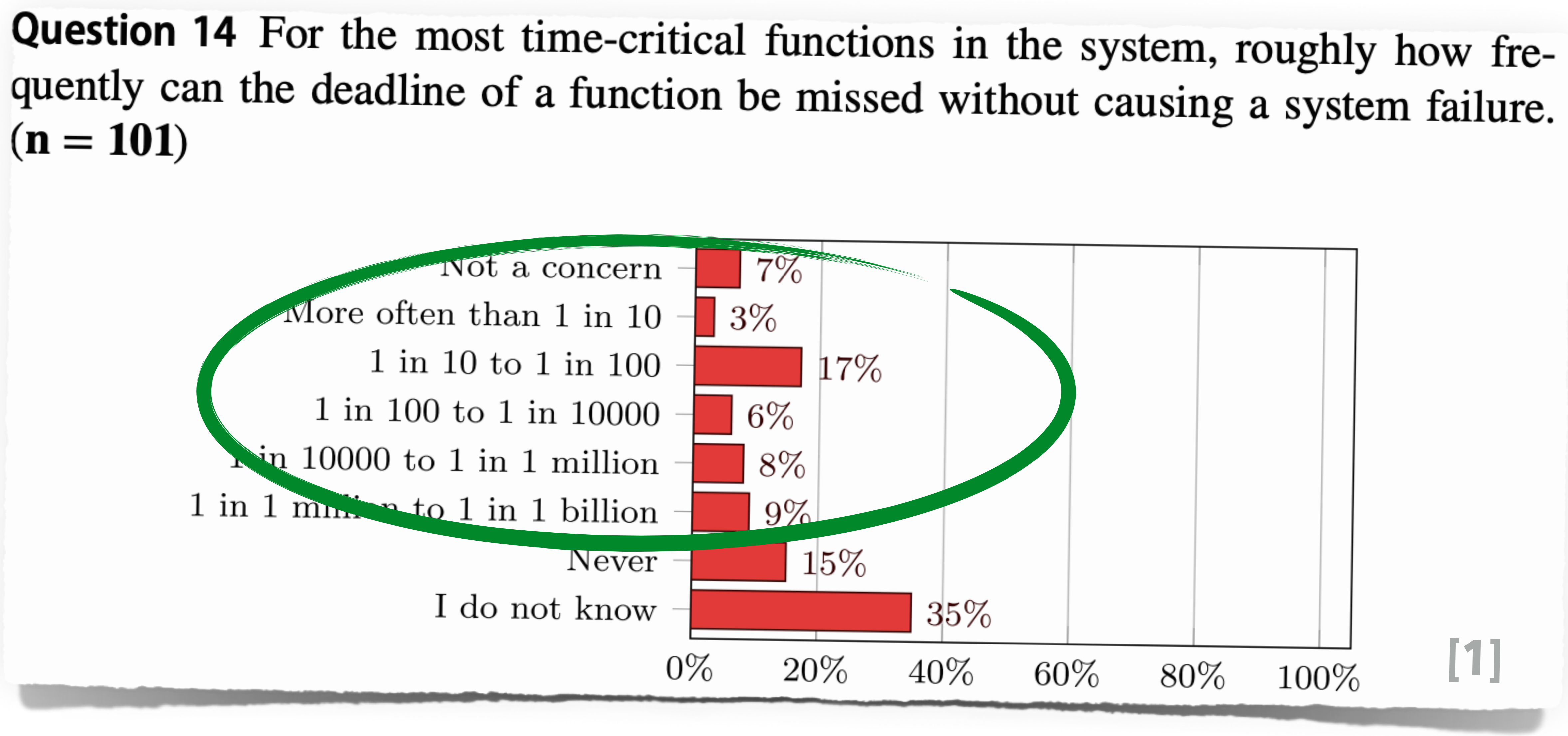
Stochastic real-time systems

➔ Model of RTSs, where workload parameters are modelled *stochastically*

Pros:

➔ Most systems **can tolerate deadline misses**

⟹ Want to take advantage of this



[1] Akesson, Benny, et al. "A comprehensive survey of industry practice in real-time systems."

THE CASE FOR STOCHASTIC RTS

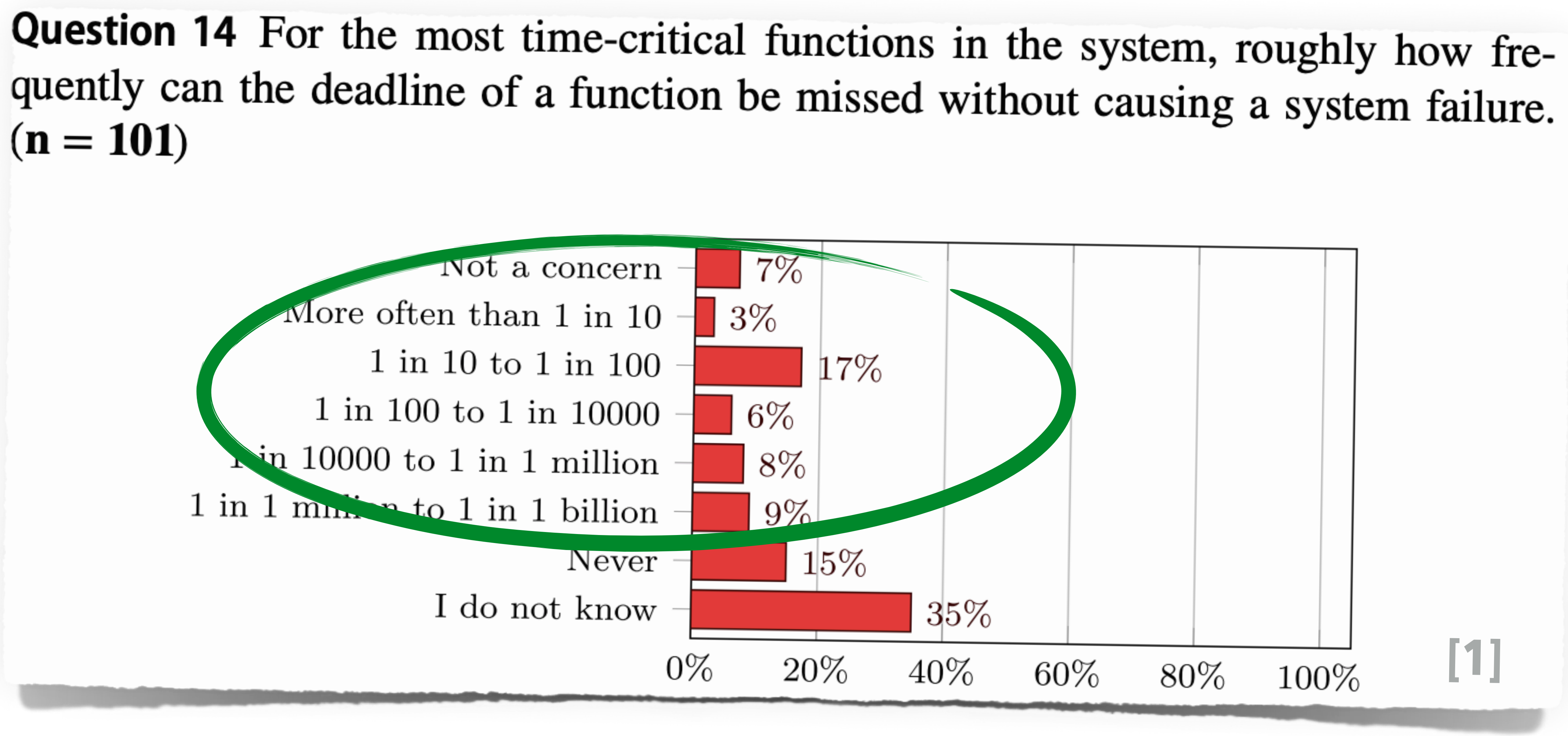
Stochastic real-time systems

➔ Model of RTSs, where workload parameters are modelled *stochastically*

Pros:

➔ Most systems **can tolerate deadline misses**
  ⟹ Want to take advantage of this

➔ Allows answering **quantitative** questions



[1] Akesson, Benny, et al. "A comprehensive survey of industry practice in real-time systems."
[2] Rivas, Juan M., et al. "Calculating latencies in an engine management system using response time analysis with MAST."

THE CASE FOR STOCHASTIC RTS

Stochastic real-time systems

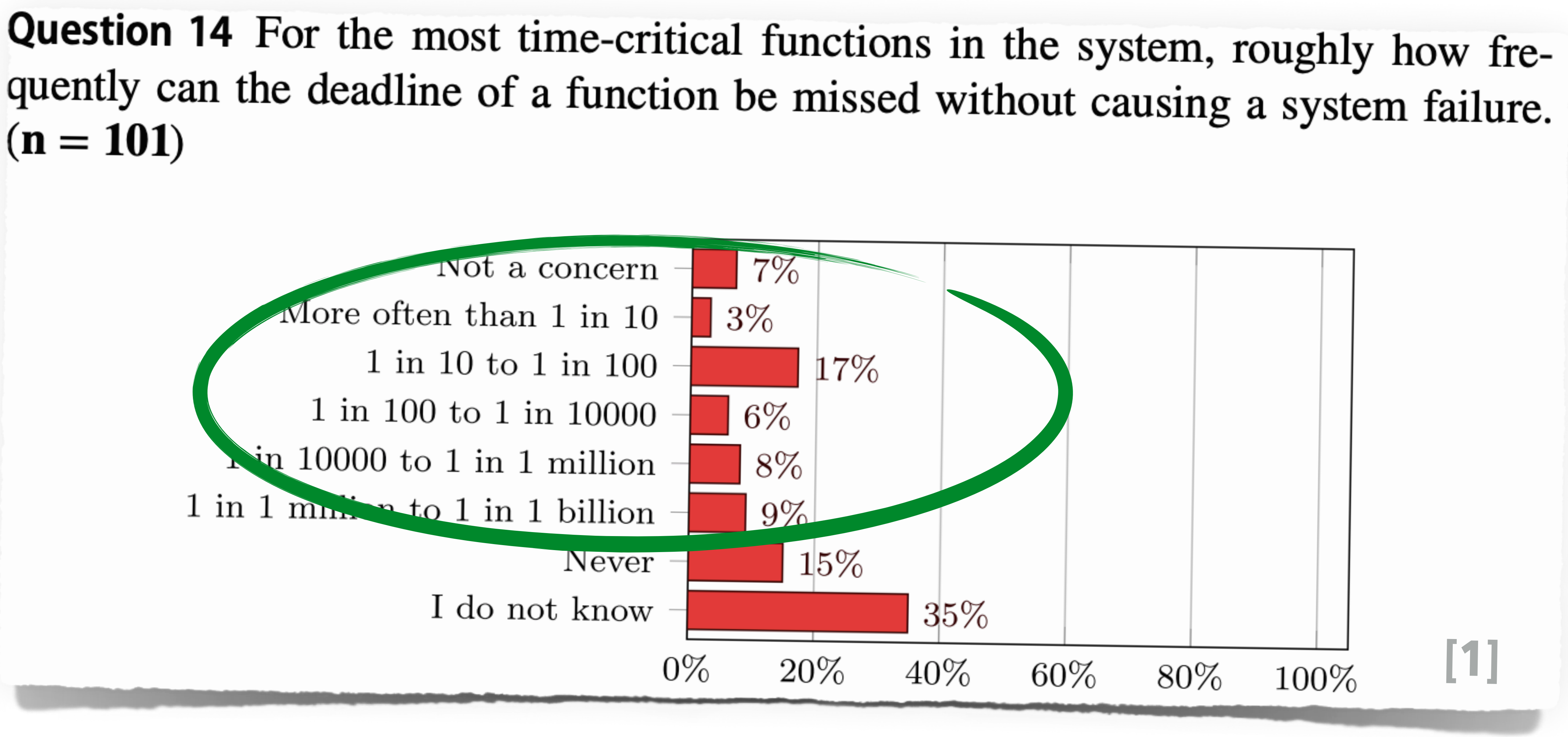
→ Model of RTSs, where workload parameters are modelled *stochastically*

Pros:

→ Most systems **can tolerate deadline misses**
  ⟹ Want to take advantage of this

→ Allows answering **quantitative** questions

→ Enables analysis of transiently **overloaded systems**
  → Ubiquitous in practice
  → *E.g., FMTV Challenge 2016*

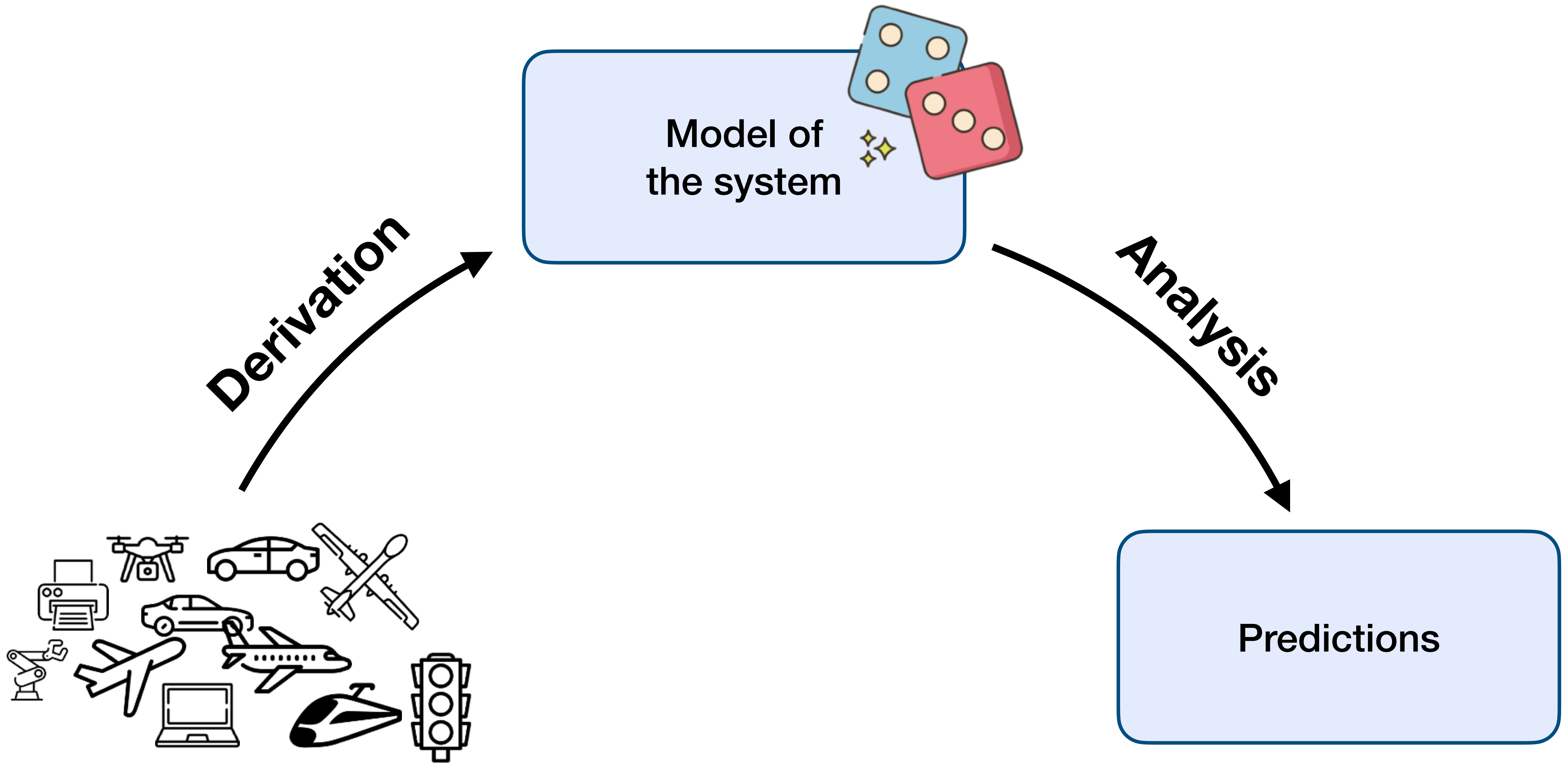


The total utilization of that system goes above 100%. Using response time analysis in such situation automatically yields unbounded (infinite) worst-case response times. [2]

[1] Akesson, Benny, et al. "A comprehensive survey of industry practice in real-time systems."
[2] Rivas, Juan M., et al. "Calculating latencies in an engine management system using response time analysis with MAST."

DEPENDENCY IN STOCHASTIC RTS

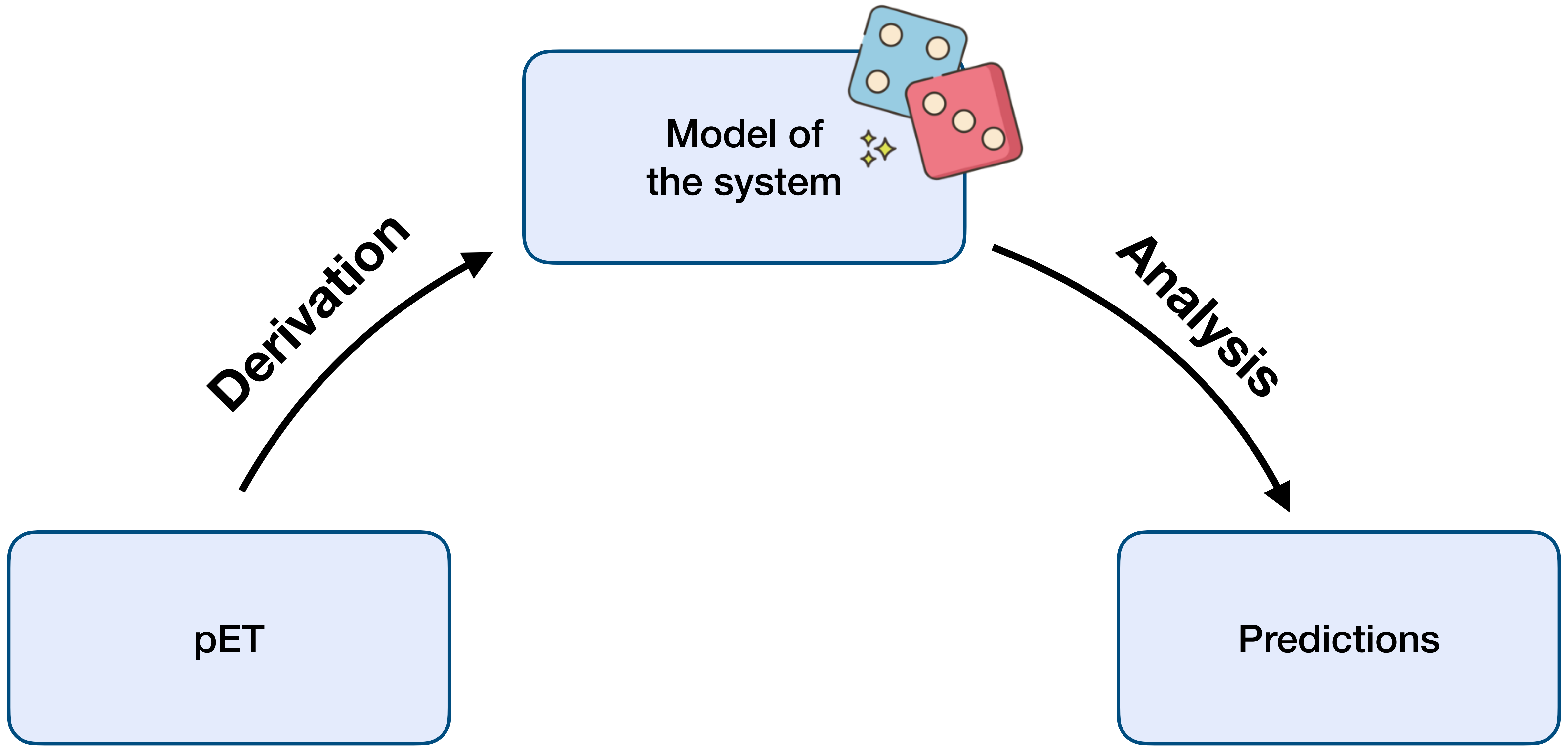
THE PROBLEM OF STOCHASTIC RTS: DEPENDENCY



THE PROBLEM OF STOCHASTIC RTS: DEPENDENCY

Probabilistic Execution Times (pETs)

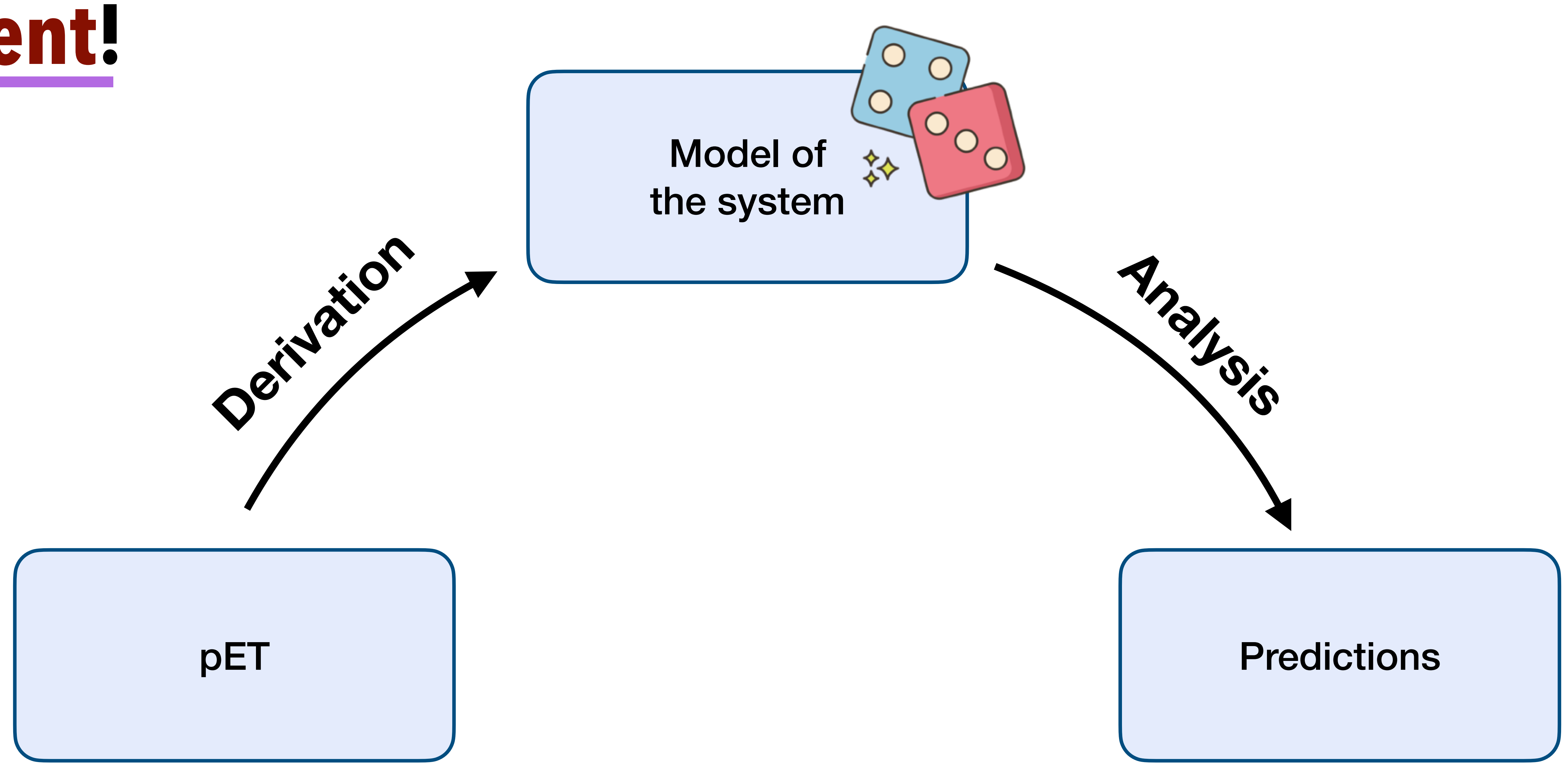
Ground-truth behavior
of jobs in the system



THE PROBLEM OF STOCHASTIC RTS: DEPENDENCY

Probabilistic Execution Times (pETs) are dependent!

Ground-truth behavior of jobs in the system

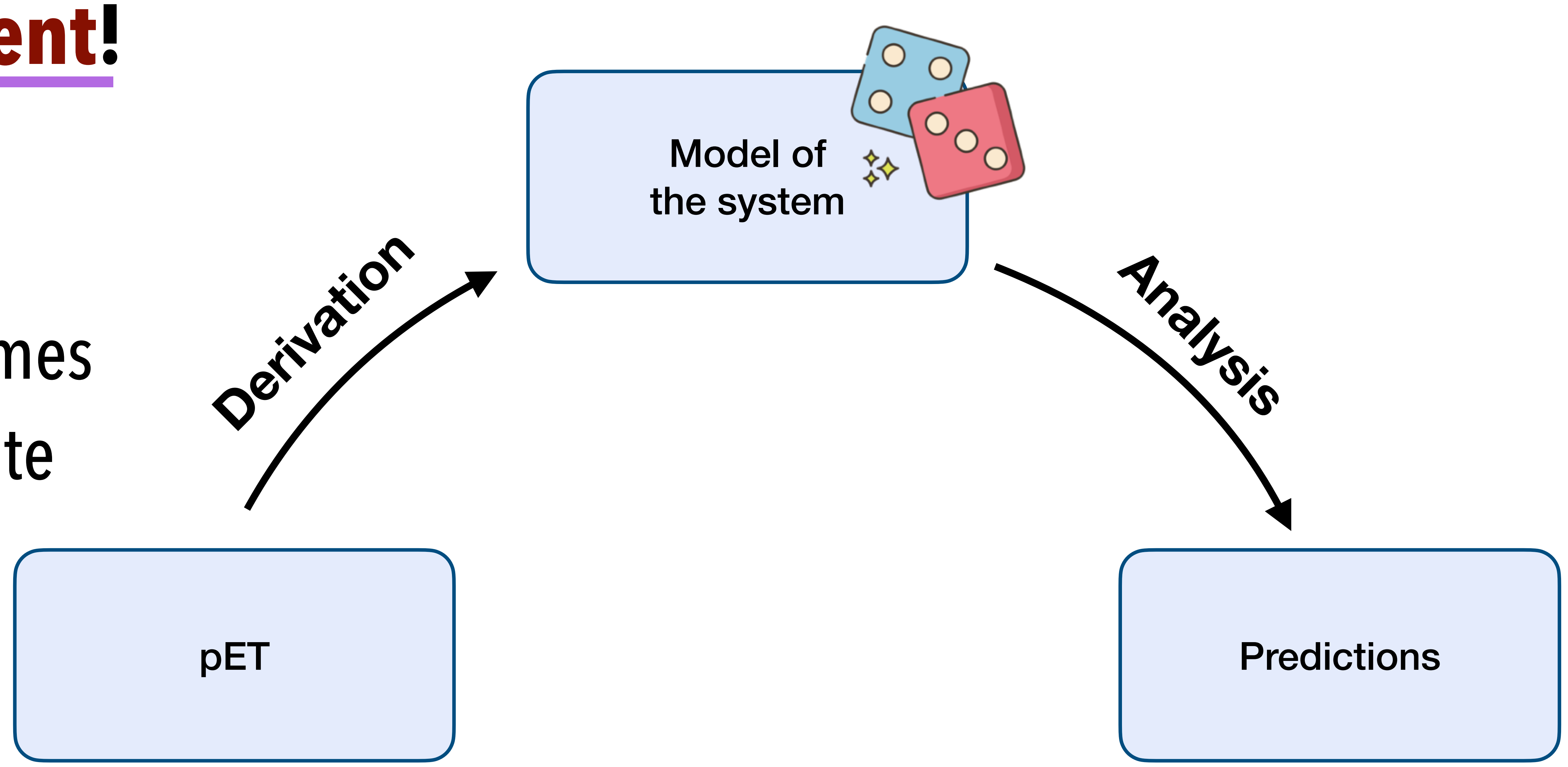


THE PROBLEM OF STOCHASTIC RTS: DEPENDENCY

Probabilistic Execution Times (pETs) are dependent!

- Image processing: Two consecutive frames might take similar amounts of compute

Ground-truth behavior of jobs in the system

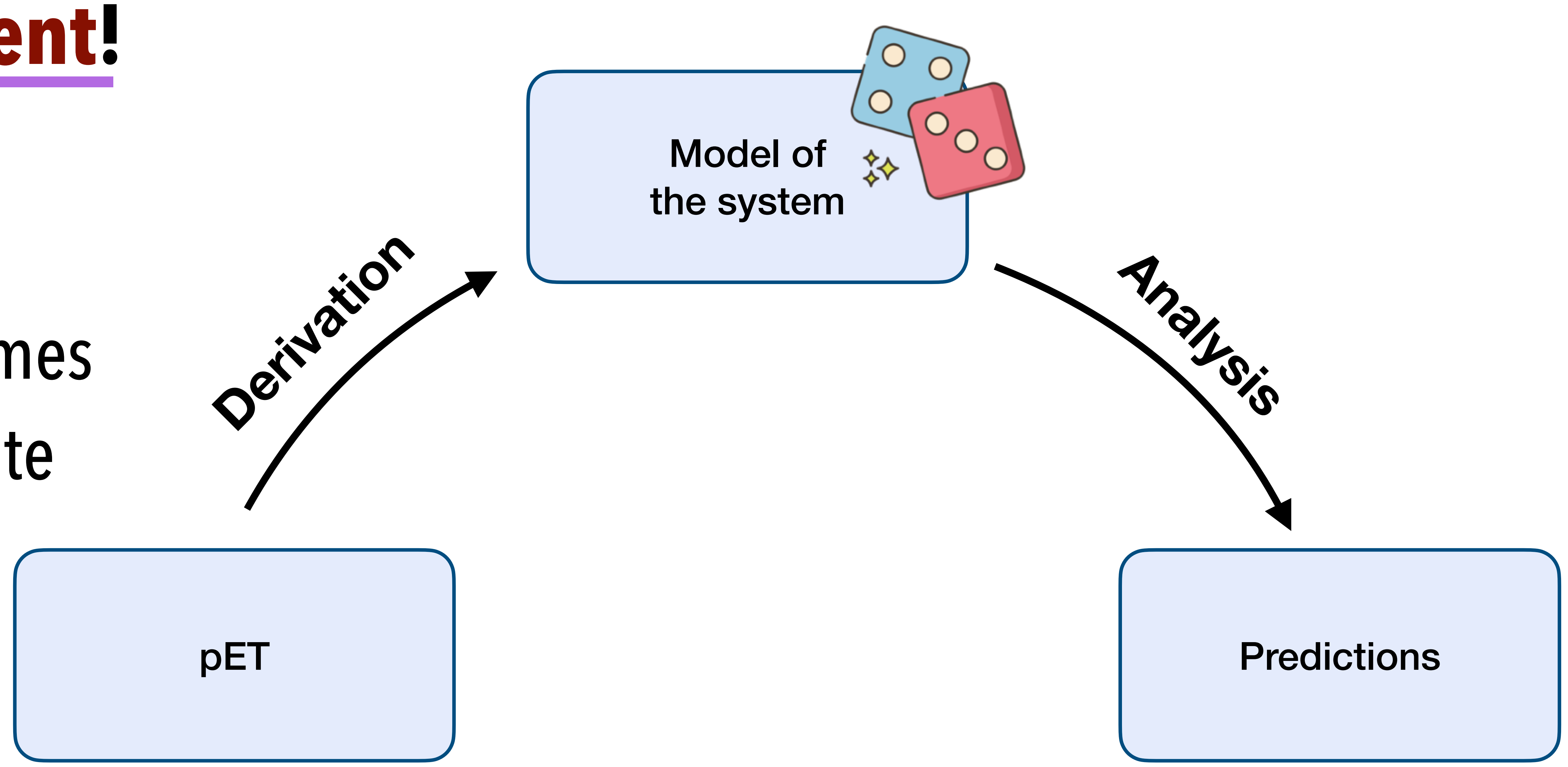


THE PROBLEM OF STOCHASTIC RTS: DEPENDENCY

Probabilistic Execution Times (pETs) are dependent!

- Image processing: Two consecutive frames might take similar amounts of compute
- Behavior of a prior job influences the state of the cache

Ground-truth behavior of jobs in the system

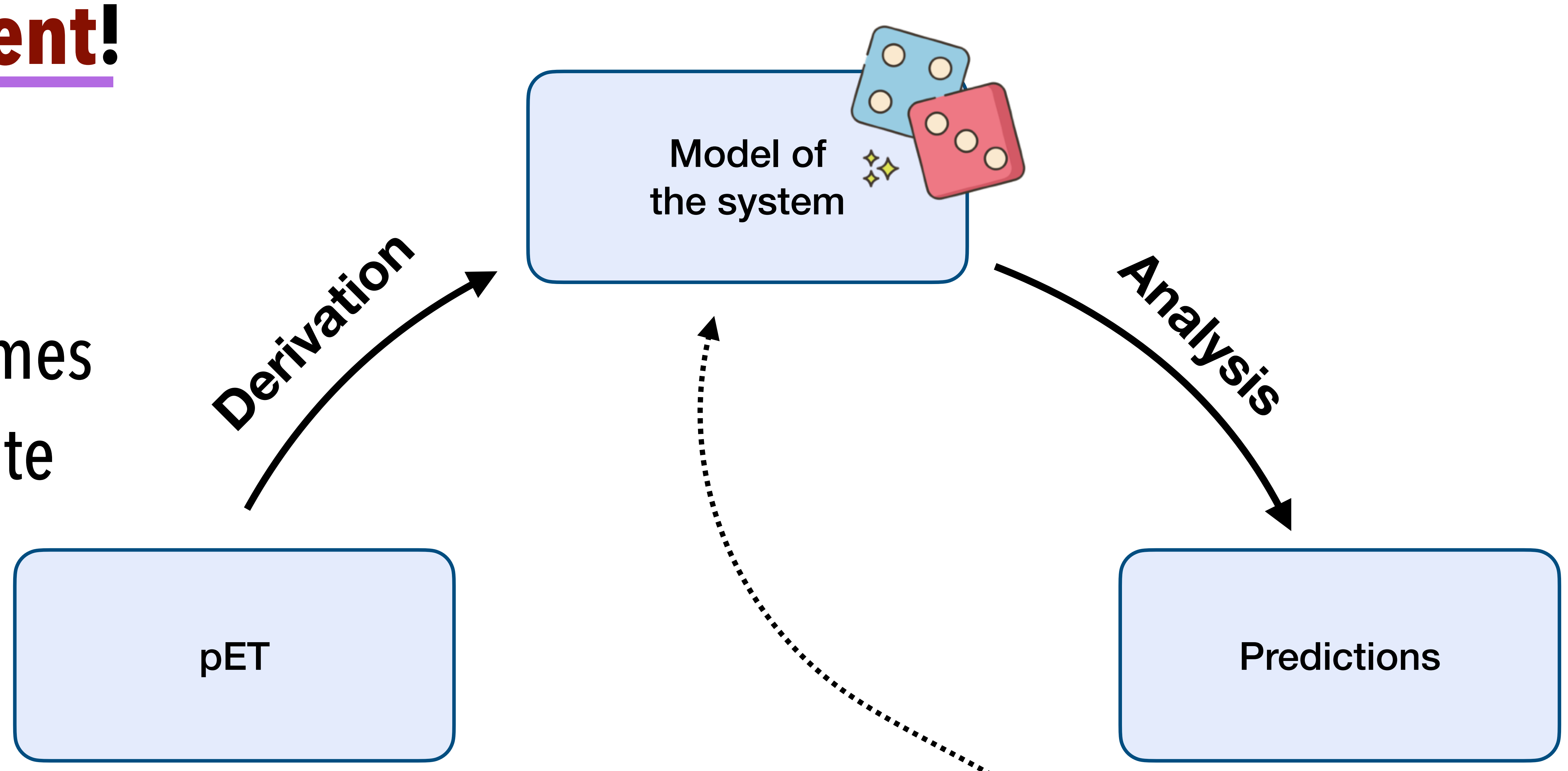


THE PROBLEM OF STOCHASTIC RTS: DEPENDENCY

Probabilistic Execution Times (pETs) are dependent!

- Image processing: Two consecutive frames might take similar amounts of compute
- Behavior of a prior job influences the state of the cache

Ground-truth behavior of jobs in the system



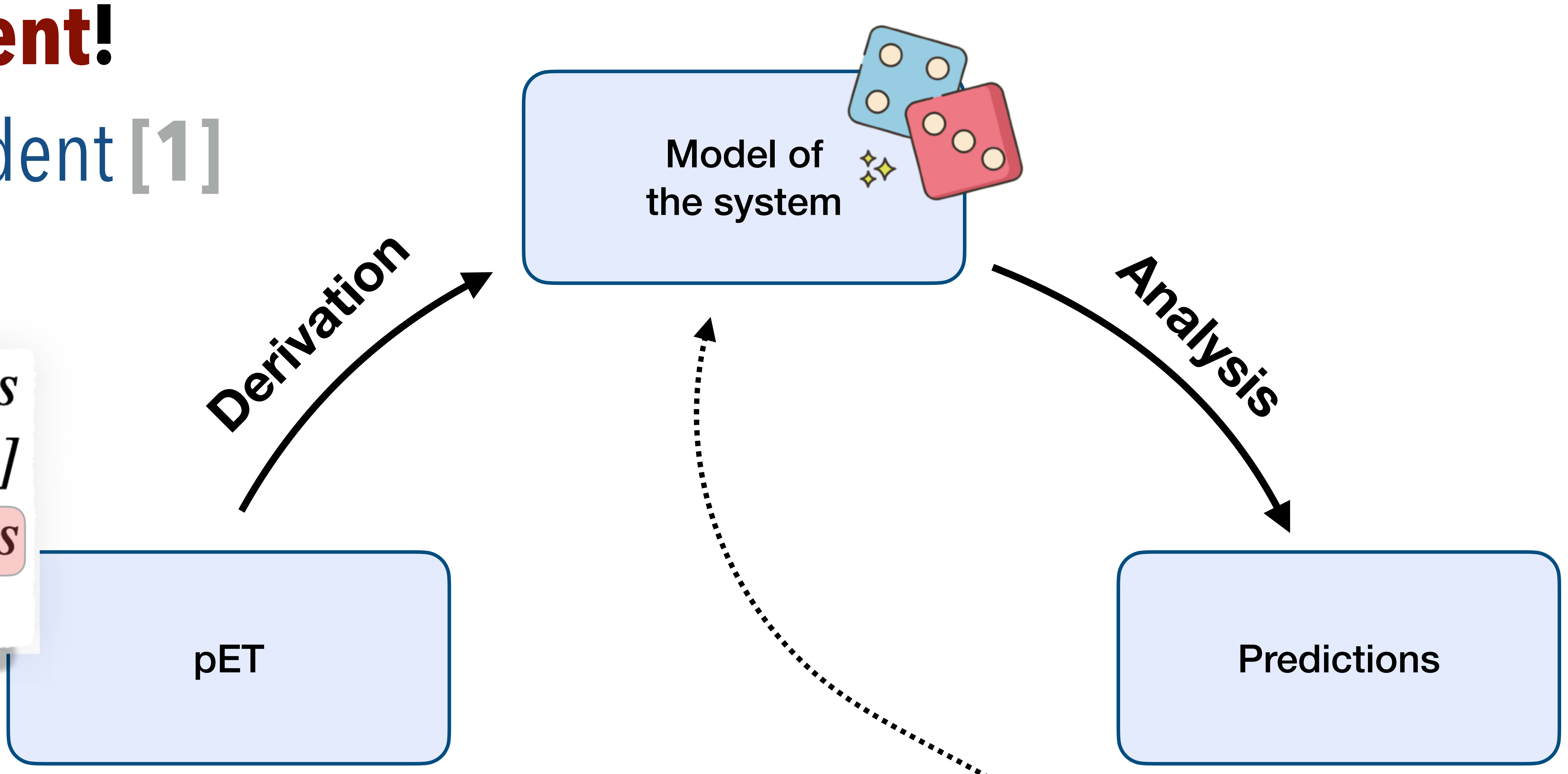
Q: Can we disregard dependency and continue anyway?

THE PROBLEM OF STOCHASTIC RTS: DEPENDENCY

Probabilistic Execution Times (pETs) are dependent!

- ➔ Tia *et al. 1995*: computation times are **not** independent [1]
  - ➔ Ignoring this fact may lead to incorrect bounds

> *"Unfortunately, the computation times of individual requests are not statistically independent. [. . .] As a consequence, the probability of meeting deadlines thus computed may be overly optimistic."*



Q: Can we disregard dependency and continue anyway?

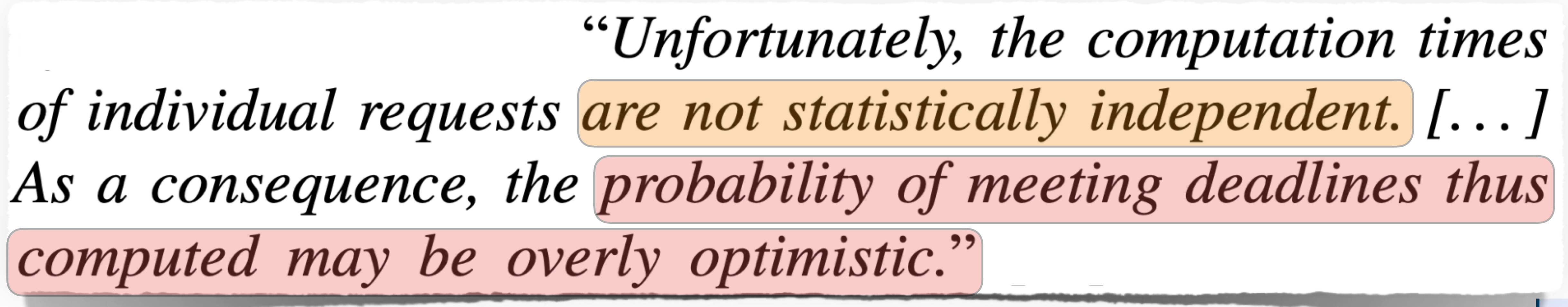
A: No, the results can be optimistic

[1] Tia, T-S., et al. "Probabilistic performance guarantee for real-time tasks with varying computation times."

THE PROBLEM OF STOCHASTIC RTS: DEPENDENCY

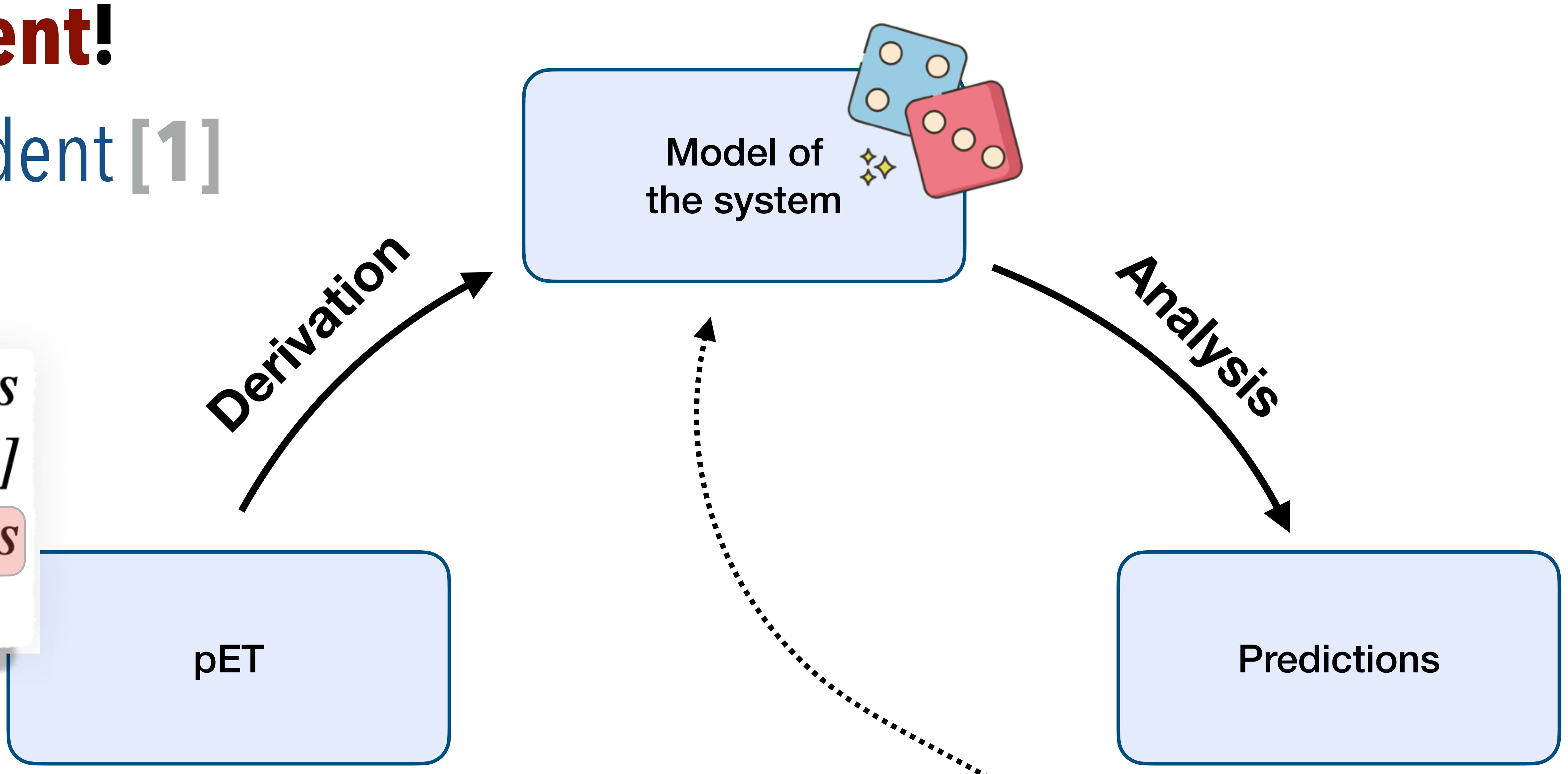
Probabilistic Execution Times (pETs) are dependent!

- ➔ Tia *et al. 1995*: computation times are **not** independent [1]
  - ➔ Ignoring this fact may lead to incorrect bounds



"Unfortunately, the computation times of individual requests are not statistically independent. [...] As a consequence, the probability of meeting deadlines thus computed may be overly optimistic."

- ➔ Limits the application of probability theory tools
  - ➔ *E.g.*, convolution is not applicable



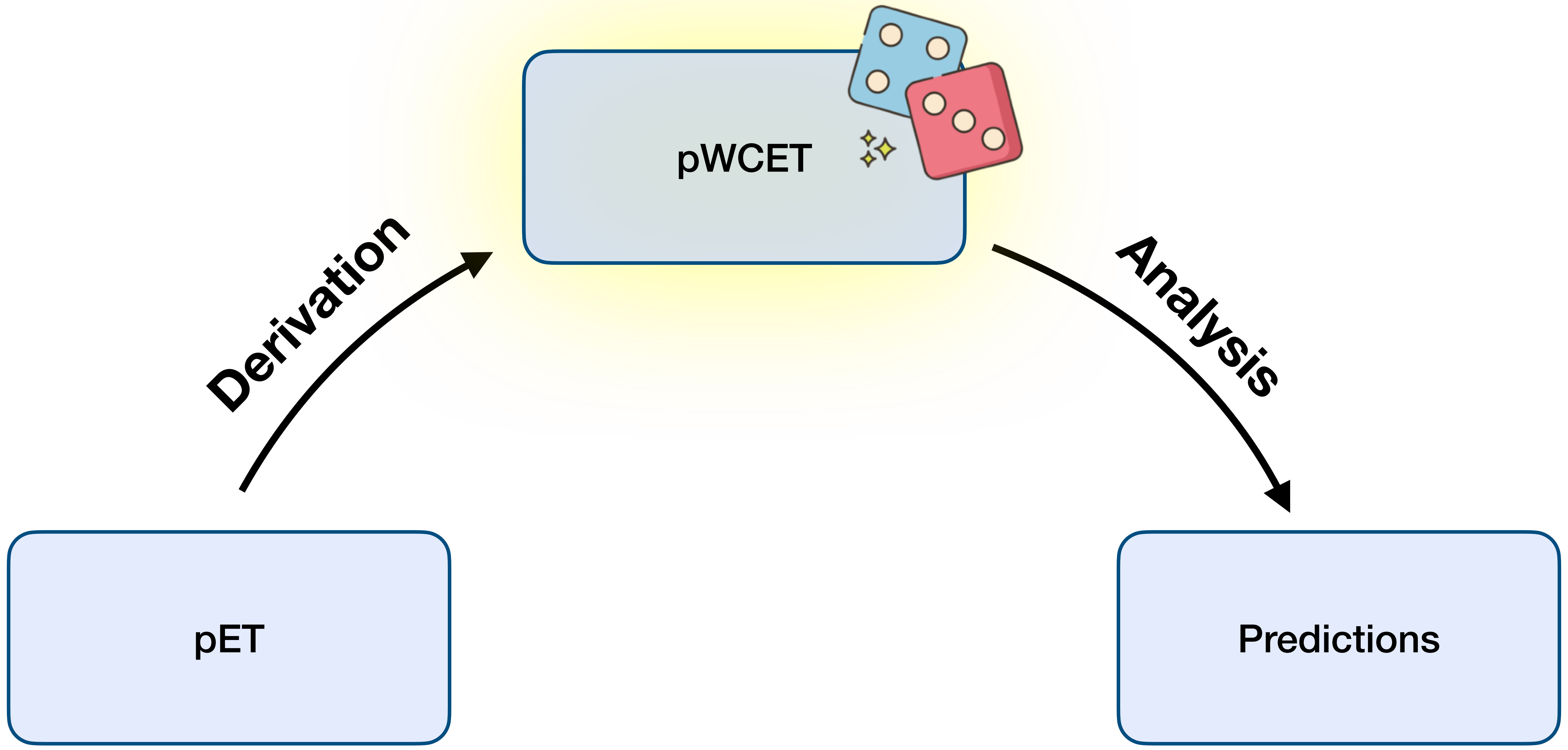
Q: Can we disregard dependency and continue anyway?

A: No, the results can be optimistic

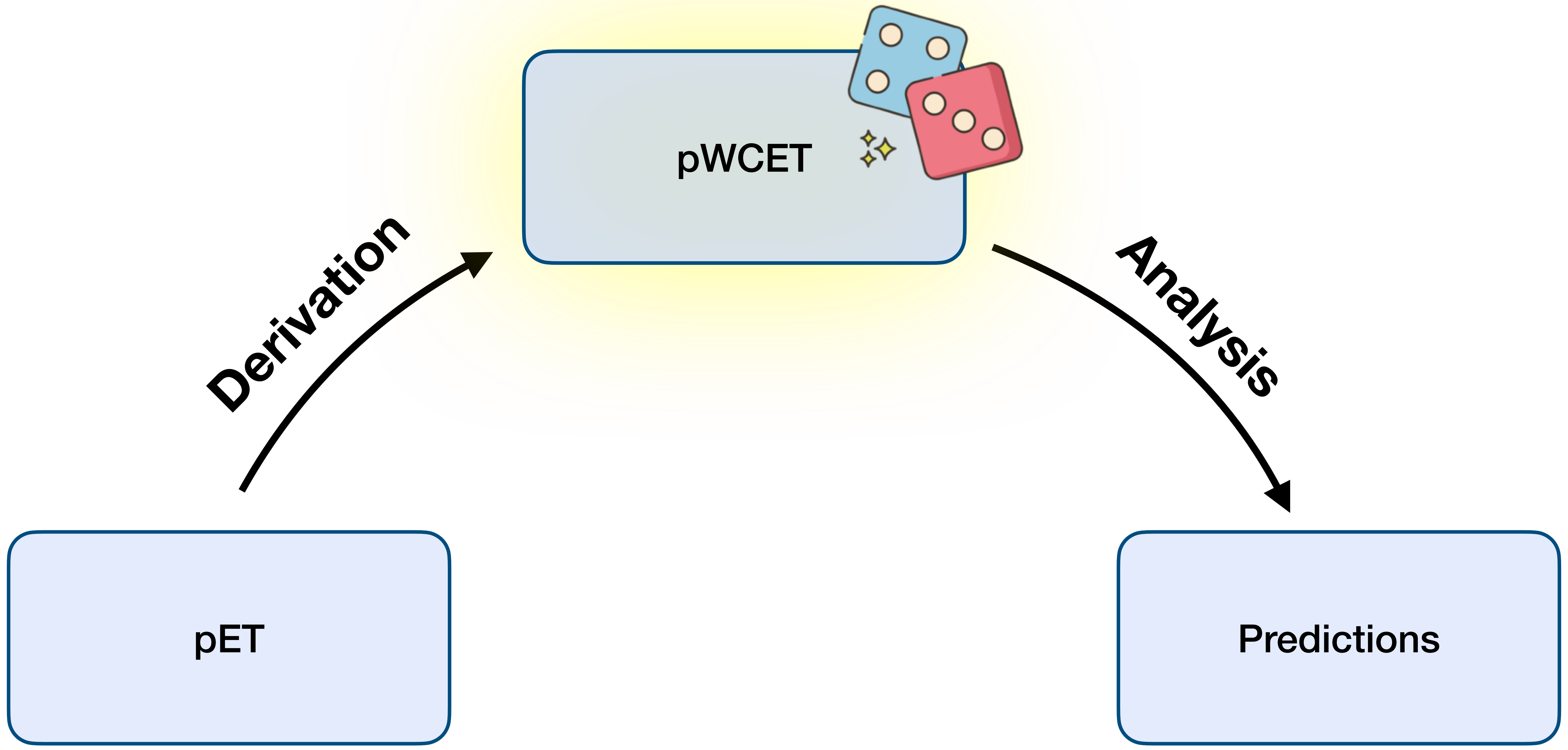
[1] Tia, T-S., et al. "Probabilistic performance guarantee for real-time tasks with varying computation times."

PRIOR WORK: pWCET

PROBABILISTIC WORST-CASE EXECUTION TIME (pWCET)



PROBABILISTIC WORST-CASE EXECUTION TIME (pWCET)

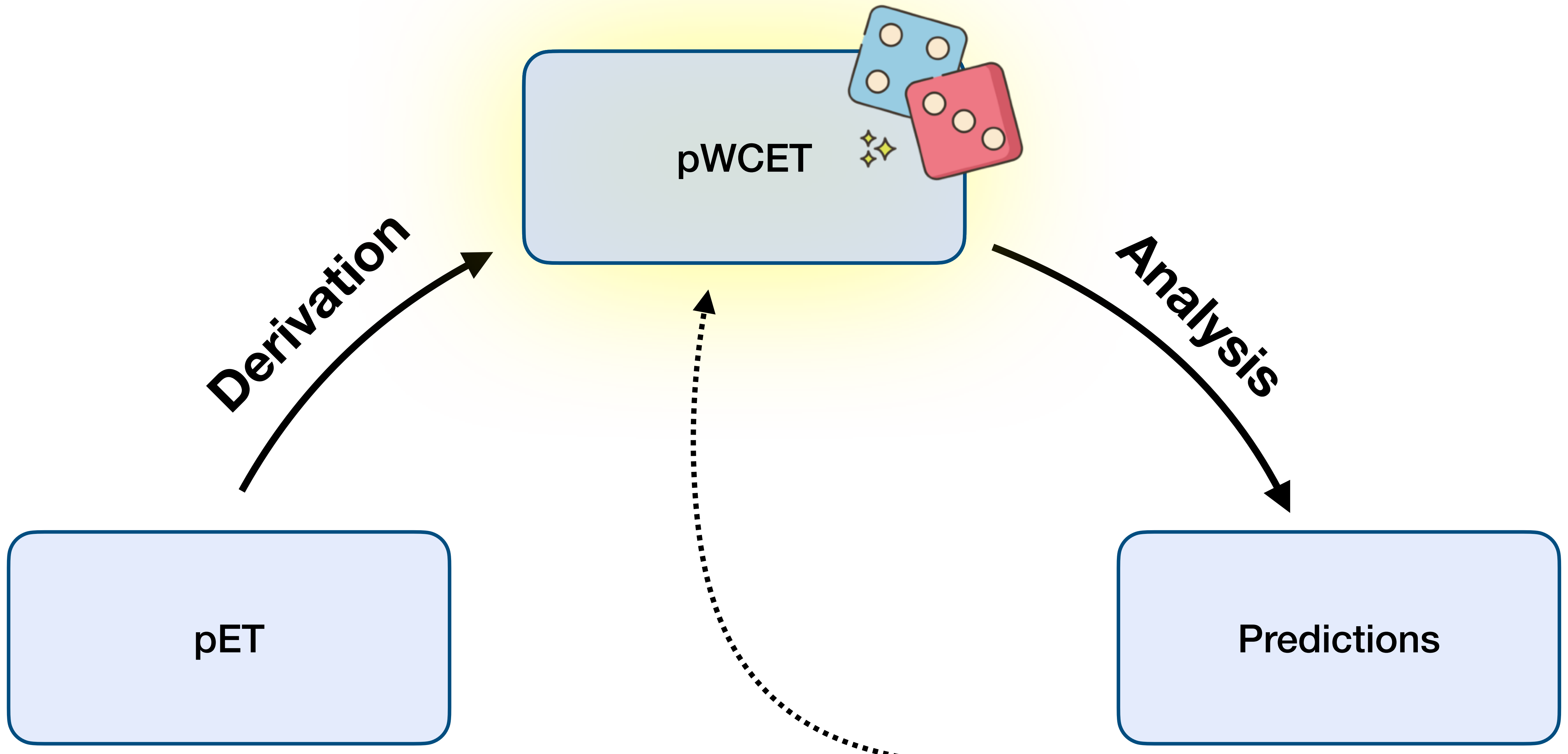


[1]

We note that the actual execution times for a sequence of jobs of a task, which exercise the same or different paths, may well show strong correlations and dependences. It is the *modelling* of the execution times via an appropriate pWCET distribution which enables probabilistic independence to be assumed. (This is similar to the conventional case of a single WCET which can similarly be used in this way, even though the actual execution times of different jobs have strong dependences).

[1] Davis, Robert Ian, and Liliana Cucu-Grosjean. "A survey of probabilistic schedulability analysis techniques for real-time systems."

PROBABILISTIC WORST-CASE EXECUTION TIME (pWCET)



[1]

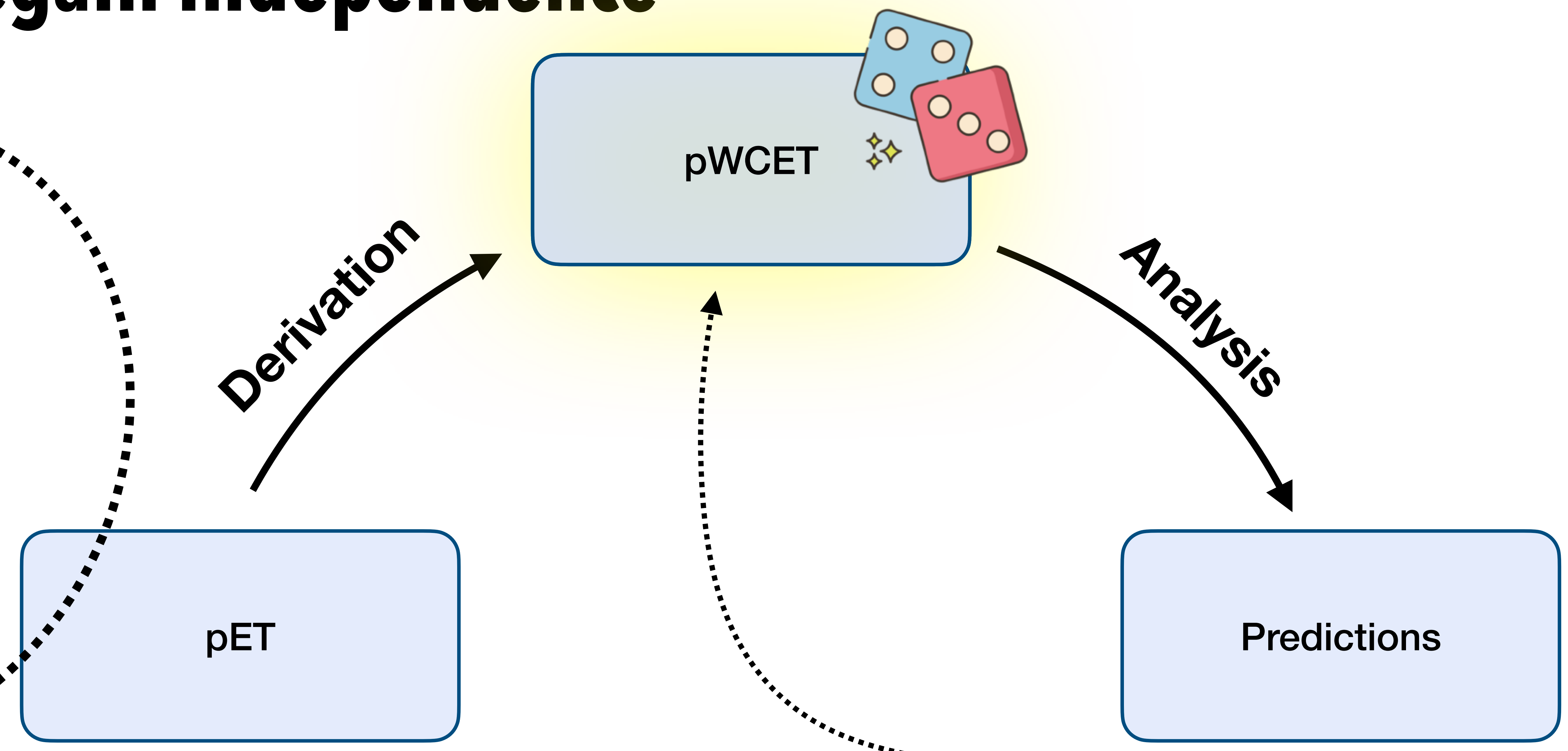
We note that the actual execution times for a sequence of jobs of a task, which exercise the same or different paths, may well show strong correlations and dependences. It is the *modelling* of the execution times via an appropriate pWCET distribution which enables probabilistic independence to be assumed. (This is similar to the conventional case of a single WCET which can similarly be used in this way, even though the actual execution times of different jobs have strong dependences).

[1] Davis, Robert Ian, and Liliana Cucu-Grosjean. "A survey of probabilistic schedulability analysis techniques for real-time systems."

PROBABILISTIC WORST-CASE EXECUTION TIME (pWCET)

pWCET is a convenient model abstraction to regain independence

➔ *Goal*: enable "IID reasoning"



Independent and identically distributed

[1]

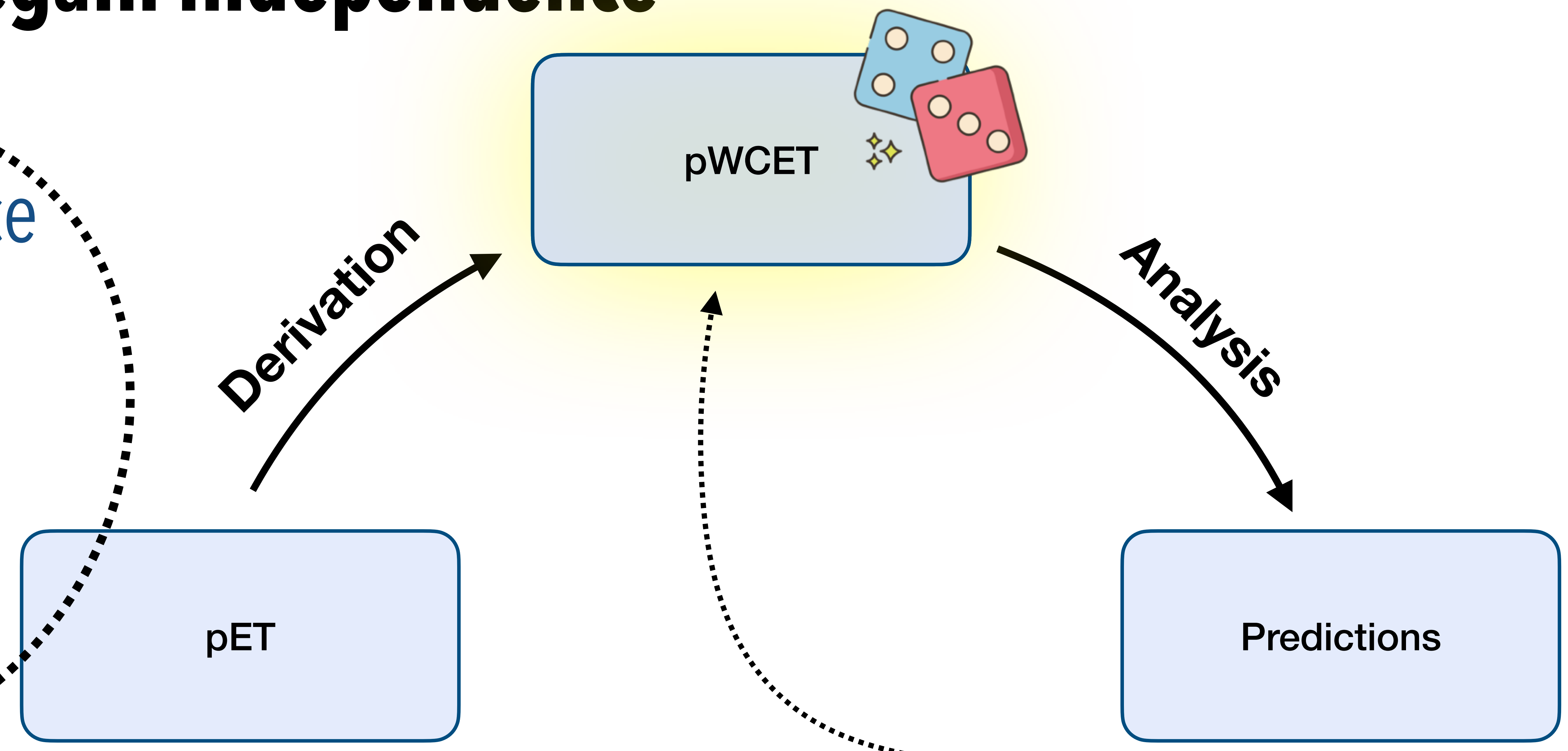
> We note that the actual execution times for a sequence of jobs of a task, which exercise the same or different paths, may well show strong correlations and dependences. It is the *modelling* of the execution times via an appropriate pWCET distribution which enables probabilistic independence to be assumed. (This is similar to the conventional case of a single WCET which can similarly be used in this way, even though the actual execution times of different jobs have strong dependences).

[1] Davis, Robert Ian, and Liliana Cucu-Grosjean. "A survey of probabilistic schedulability analysis techniques for real-time systems."

PROBABILISTIC WORST-CASE EXECUTION TIME (pWCET)

pWCET is a convenient model abstraction to regain independence

- ➔ *Goal*: enable "IID reasoning"
- ➔ The **mainstream** approach to hiding dependence
- ➔ Unlocks powerful probability theory techniques
  - ➔ Such as *convolution*, *Chernoff bound*, *etc.*



Independent and identically distributed

[1]

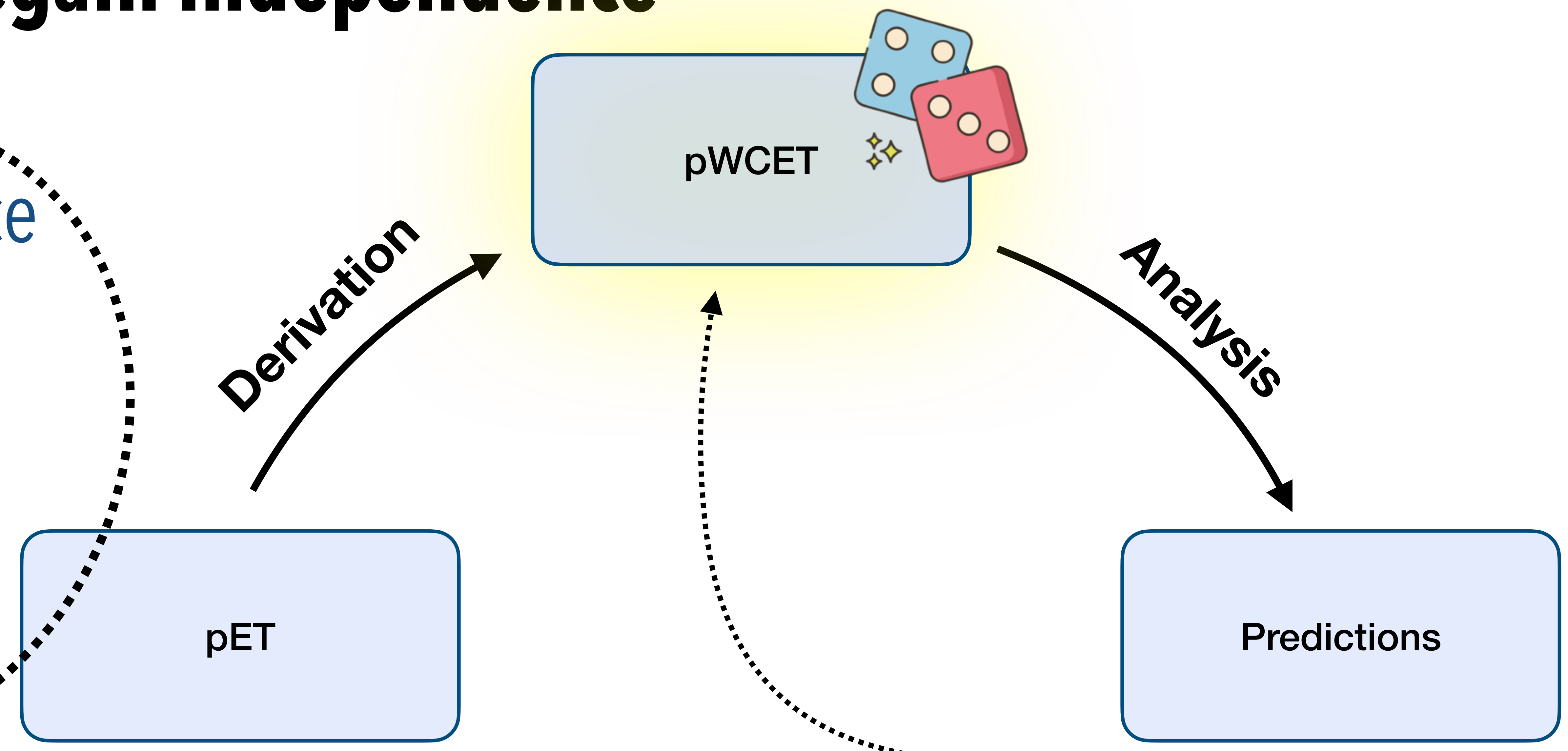
We note that the actual execution times for a sequence of jobs of a task, which exercise the same or different paths, may well show strong correlations and dependences. It is the *modelling* of the execution times via an appropriate pWCET distribution which enables probabilistic independence to be assumed. (This is similar to the conventional case of a single WCET which can similarly be used in this way, even though the actual execution times of different jobs have strong dependences).

[1] Davis, Robert Ian, and Liliana Cucu-Grosjean. "A survey of probabilistic schedulability analysis techniques for real-time systems."

PROBABILISTIC WORST-CASE EXECUTION TIME (pWCET)

pWCET is a convenient model abstraction to regain independence

- ➔ *Goal*: enable "IID reasoning"
- ➔ The **mainstream** approach to hiding dependence
- ➔ Unlocks powerful probability theory techniques
  - ➔ Such as *convolution*, *Chernoff bound*, *etc.*
- ➔ .... but when **exactly** is a pWCET distribution "appropriate"?



Independent and identically distributed

[1]

We note that the actual execution times for a sequence of jobs of a task, which exercise the same or different paths, may well show strong correlations and dependences. It is the *modelling* of the execution times via an appropriate pWCET distribution which enables probabilistic independence to be assumed. (This is similar to the conventional case of a single WCET which can similarly be used in this way, even though the actual execution times of different jobs have strong dependences).

[1] Davis, Robert Ian, and Liliana Cucu-Grosjean. "A survey of probabilistic schedulability analysis techniques for real-time systems."

THE STATE-OF-THE-ART pWCET DEFINITION

▶ **Definition 2.** The *probabilistic Worst-Case Execution Time (pWCET)* distribution for a task is the least upper bound, in the sense of the greater than or equal to operator $\succeq$ (defined below), on the execution time distribution of the jobs of the task for every valid scenario of operation, where a *scenario* of operation is defined as an infinitely repeating sequence of input states (including both input values and software state variables) and initial hardware states that characterise a feasible way in which recurrent execution of the task may occur. [1]

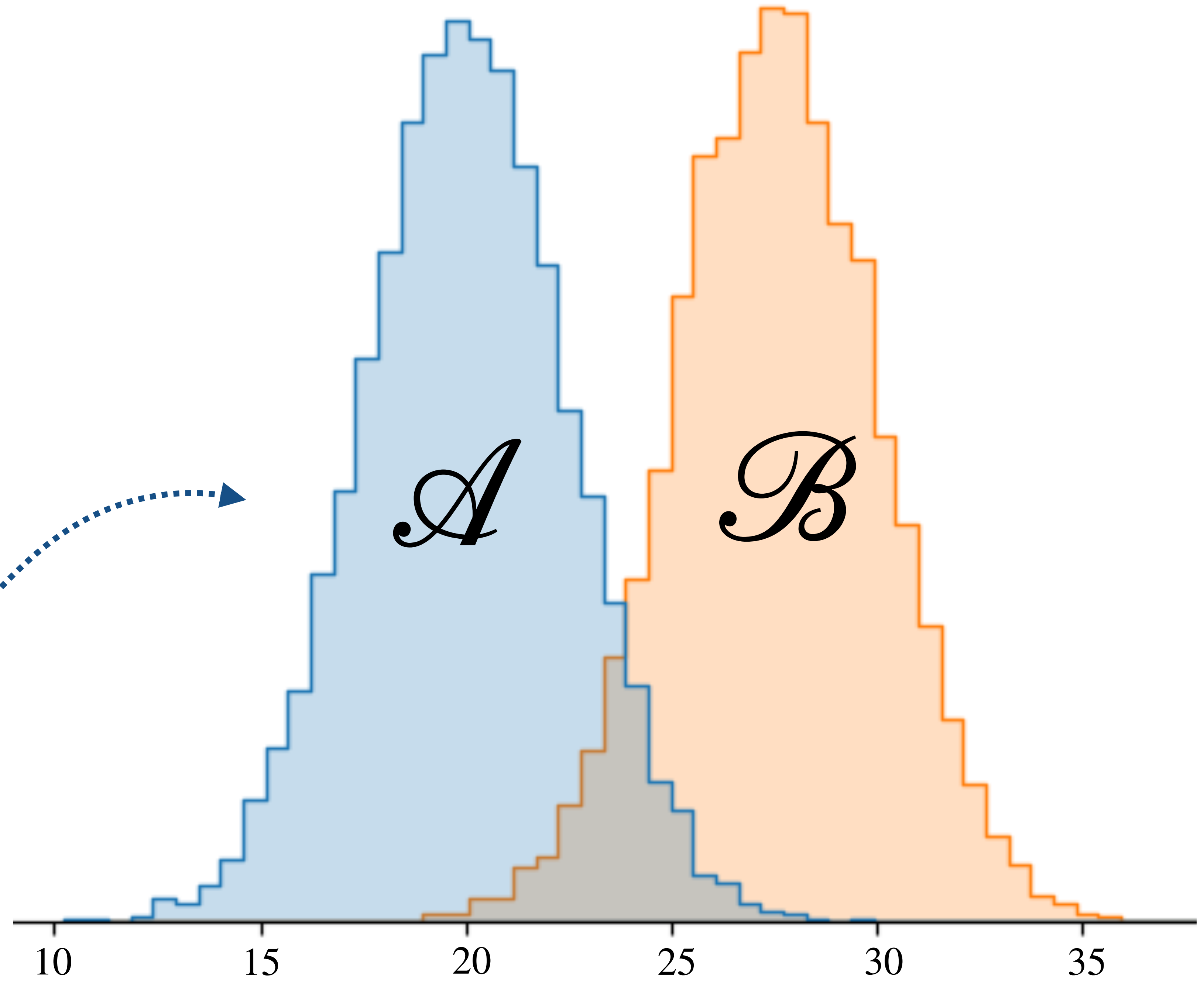
[1] Davis, Robert Ian, and Liliana Cucu-Grosjean. "A survey of probabilistic schedulability analysis techniques for real-time systems."

THE STATE-OF-THE-ART pWCET DEFINITION

▶ **Definition 2.** The *probabilistic Worst-Case Execution Time (pWCET)* distributi… r a task is the least upper bound, in the sense of the greater than or equal to operator $\succeq$ (… elow), on the execution time distribution of the jobs of the task for every valid scenario of operation, where a *scenario* of operation is defined as an infinitely repeating sequence of input states (including both input values and software state variables) and initial hardware states that characterise a feasible way in which recurrent execution of the task may occur. [1]

Side note: dominance relation $\preceq$

- ➔ Proposed by Diaz *et al.* in 2004 [2]
- ➔ Partial order on random variables
  - ➔ Similar to stochastic dominance
- ➔ $\mathscr{A} \preceq \mathscr{B} := \forall x, \mathbb{P}[\mathscr{A} \leq x] \geq \mathbb{P}[\mathscr{B} \leq x]$



[1] Davis, Robert Ian, and Liliana Cucu-Grosjean. "A survey of probabilistic schedulability analysis techniques for real-time systems."
[2] Diaz, Jose Luis, et al. "Pessimism in the stochastic analysis of real-time systems: Concept and applications."

THE STATE-OF-THE-ART pWCET DEFINITION

▶ **Definition 2.** The *probabilistic Worst-Case Execution Time (pWCET)* distribution for a task is the least upper bound, in the sense of the greater than or equal to operator $\succeq$ (defined below), on the execution time distribution of the jobs of the task for every valid scenario of operation, where a *scenario* of operation is defined as an infinitely repeating sequence of input states (including both input values and software state variables) and initial hardware states that characterise a feasible way in which recurrent execution of the task may occur. [1]

Pros

- ➔ Gives the right intuition
- ➔ Identifies that "scenario of operation" is the key notion

[1] Davis, Robert Ian, and Liliana Cucu-Grosjean. "A survey of probabilistic schedulability analysis techniques for real-time systems."

pWCET DEFINITION IS OPEN TO INTERPRETATION

▶ **Definition 2.** The *probabilistic Worst-Case Execution Time (pWCET)* distribution for a task is the least upper bound, in the sense of the greater than or equal to operator $\succeq$ (defined below), on the execution time distribution of the jobs of the task for every valid scenario of operation, where a *scenario* of operation is defined as an infinitely repeating sequence of input states (including both input values and software state variables) and initial hardware states that characterise a feasible way in which recurrent execution of the task may occur. [1]

Pros

➔ Gives the right intuition

➔ Identifies that "scenario of operation" is the key notion

Cons

➔ Open to interpretation 🤔

- ➔ Key aspects are stated in **prose** only
- ➔ **Not** suitable for formal verification

[1] Davis, Robert Ian, and Liliana Cucu-Grosjean. "A survey of probabilistic schedulability analysis techniques for real-time systems."

pWCET DEFINITION IS OPEN TO INTERPRETATION

▶ **Definition 2.** The *probabilistic Worst-Case Execution Time (pWCET)* distribution for a task is the least upper bound, in the sense of the greater than or equal to operator $\succeq$ (defined below), on the execution time distribution of the jobs of the task for every valid scenario of operation, where a *scenario* of operation is defined as an infinitely repeating sequence of input states (including both input values and software state variables) and initial hardware states that characterise a feasible way in which recurrent execution of the task may occur. [1]

Pros

- ➔ Gives the right intuition
- ➔ Identifies that "scenario of operation" is the key notion

Cons

- ➔ Open to interpretation 🤔
  - ➔ Key aspects are stated in **prose** only
  - ➔ **Not** suitable for formal verification
- ➔ **Does not** necessarily enable IID-based analyses

[1] Davis, Robert Ian, and Liliana Cucu-Grosjean. "A survey of probabilistic schedulability analysis techniques for real-time systems."

SOTA pWCET *DOES NOT* ENABLE IID ANALYSIS

Already noted in [1]

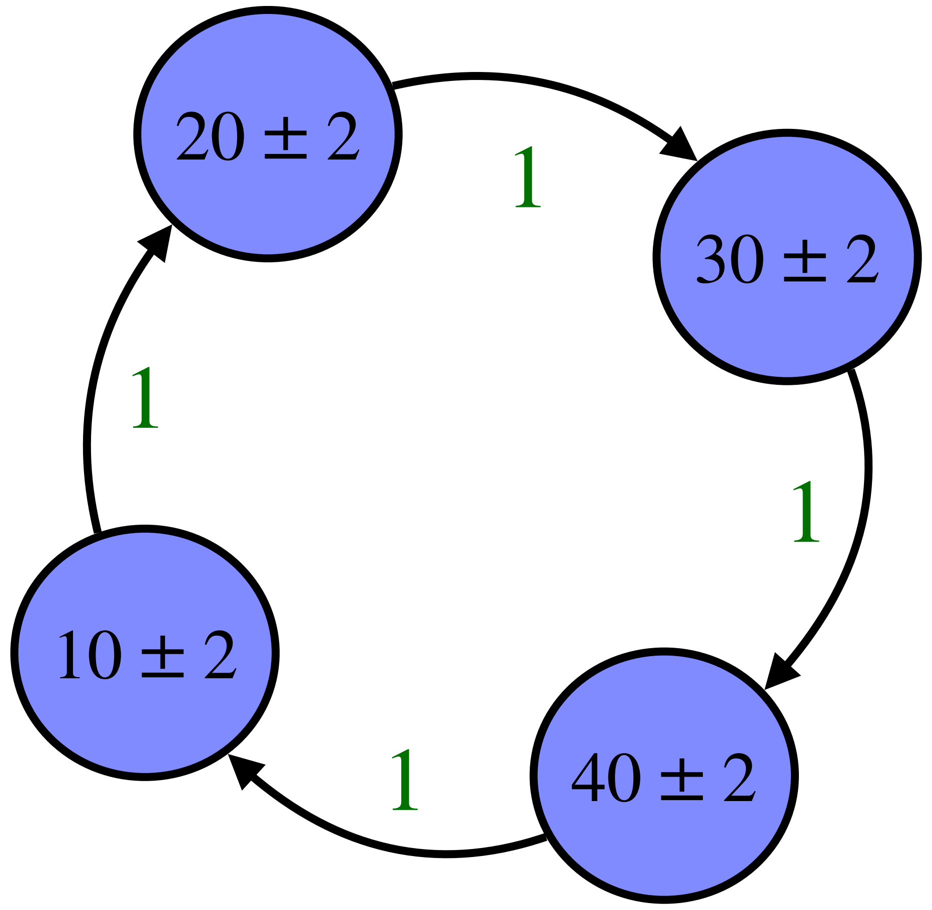
[1] Davis, Robert Ian, and Liliana Cucu-Grosjean. "A survey of probabilistic timing analysis techniques for real-time systems."

SOTA pWCET *DOES NOT* ENABLE IID ANALYSIS

Already noted in [1]

A toy system: [1]

- ➔ Time-predictable hardware
- ➔ System has **four** states
- ➔ State **cycling through** its four possible values
- ➔ Small variability in each of the states
- ➔ Starts with random state



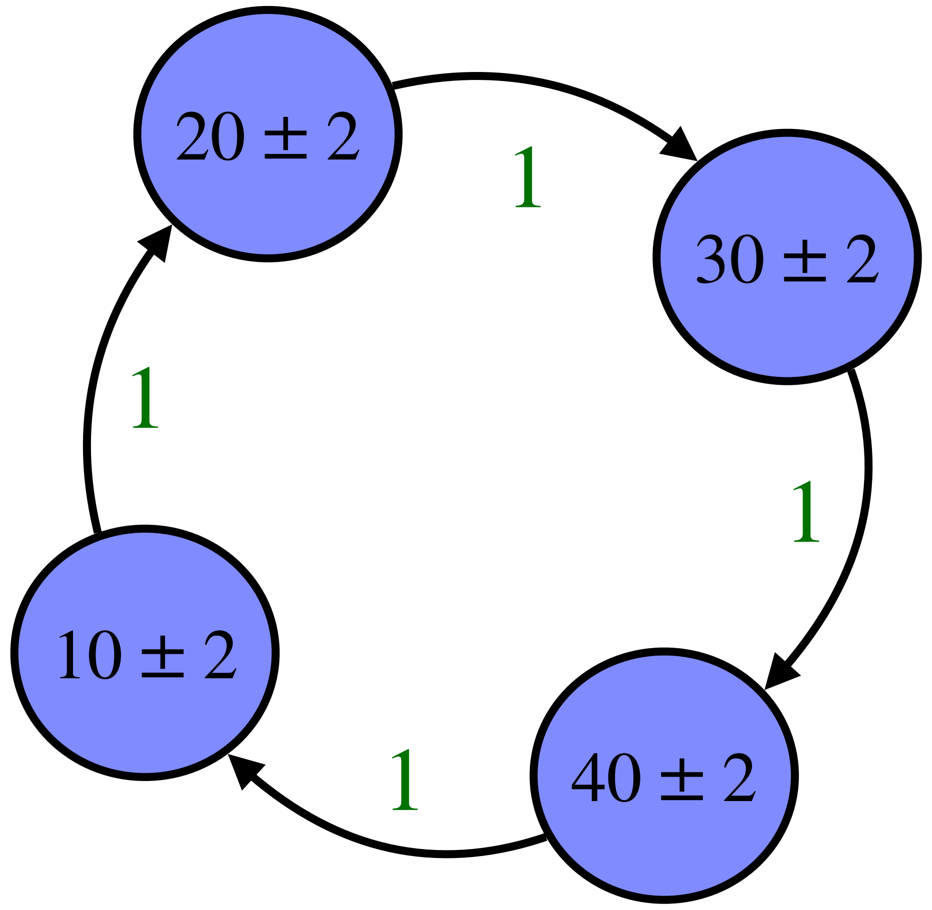
[1] Davis, Robert Ian, and Liliana Cucu-Grosjean. "A survey of probabilistic timing analysis techniques for real-time systems."

SOTA pWCET *DOES NOT* ENABLE IID ANALYSIS

Already noted in [1]

A toy system: [1]

- Time-predictable hardware
- System has **four** states
- State **cycling through** its four possible values
- Small variability in each of the states
- Starts with random state



- Resulting pET distribution: [1]

$$\begin{pmatrix} 10 \pm 2 & 20 \pm 2 & 30 \pm 2 & 40 \pm 2 \\ 1/4 & 1/4 & 1/4 & 1/4 \end{pmatrix}$$

- Valid pWCET distribution: [1]

$$\begin{pmatrix} 12 & 22 & 32 & 42 \\ 1/4 & 1/4 & 1/4 & 1/4 \end{pmatrix}$$

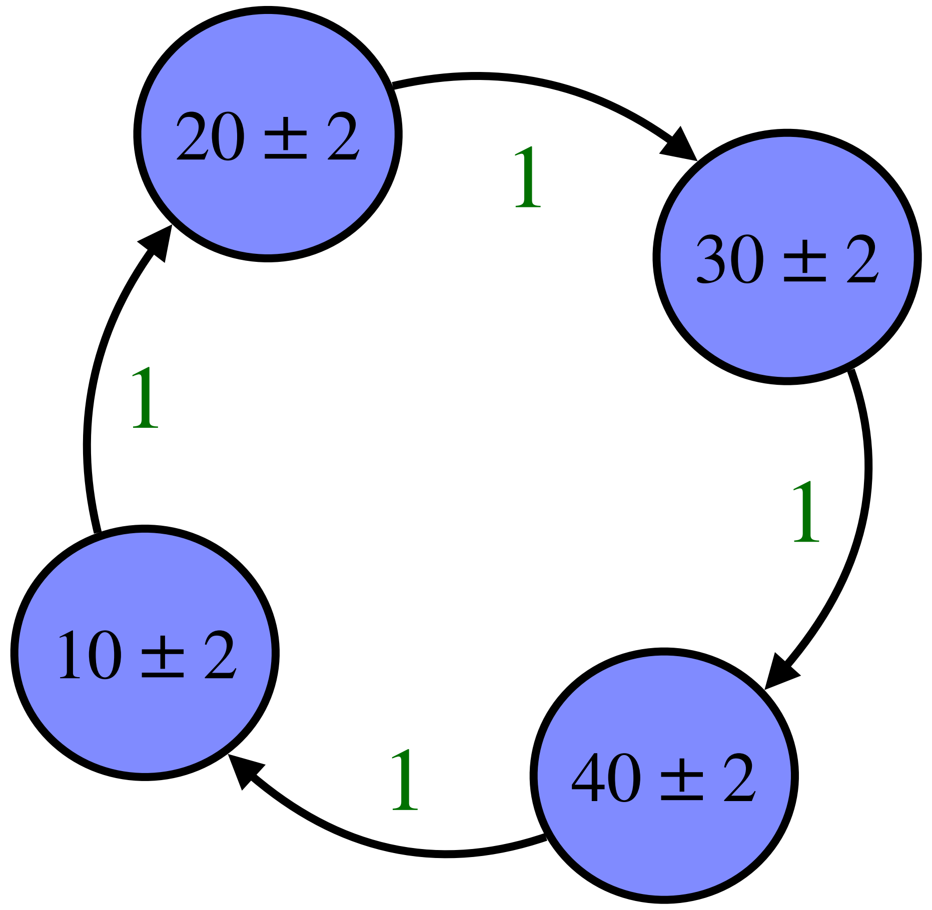
[1] Davis, Robert Ian, and Liliana Cucu-Grosjean. "A survey of probabilistic timing analysis techniques for real-time systems."

SOTA pWCET *DOES NOT* ENABLE IID ANALYSIS

Already noted in [1]

A toy system: [1]

- Time-predictable hardware
- System has **four** states
- State **cycling through** its four possible values
- Small variability in each of the states
- Starts with random state



- Resulting pET distribution: [1]

$$\begin{pmatrix} 10 \pm 2 & 20 \pm 2 & 30 \pm 2 & 40 \pm 2 \\ 1/4 & 1/4 & 1/4 & 1/4 \end{pmatrix}$$

- Valid pWCET distribution: [1]

$$\begin{pmatrix} 12 & 22 & 32 & 42 \\ 1/4 & 1/4 & 1/4 & 1/4 \end{pmatrix}$$

Except that ....

- Smallest workload of four consecutive jobs:
  - $(10 - 2) + (20 - 2) + (30 - 2) + (40 - 2) = 92$

$$\mathbb{P}\left[\sum_4 \text{pET} \geq 92\right] = 1$$

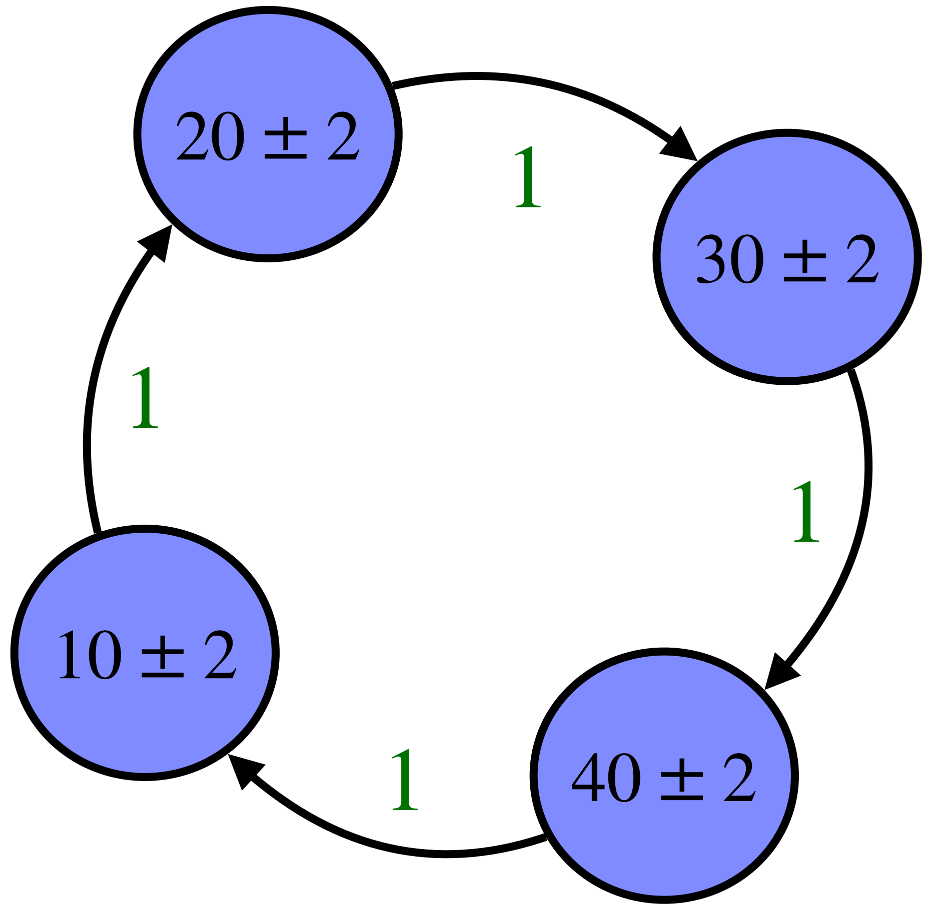
[1] Davis, Robert Ian, and Liliana Cucu-Grosjean. "A survey of probabilistic timing analysis techniques for real-time systems."

SOTA pWCET *DOES NOT* ENABLE IID ANALYSIS

Already noted in [1]

A toy system: [1]

- Time-predictable hardware
- System has **four** states
- State **cycling through** its four possible values
- Small variability in each of the states
- Starts with random state



- Resulting pET distribution: [1]

$$\begin{pmatrix} 10 \pm 2 & 20 \pm 2 & 30 \pm 2 & 40 \pm 2 \\ 1/4 & 1/4 & 1/4 & 1/4 \end{pmatrix}$$

- Valid pWCET distribution: [1]

$$\begin{pmatrix} 12 & 22 & 32 & 42 \\ 1/4 & 1/4 & 1/4 & 1/4 \end{pmatrix}$$

Except that ....

- Smallest workload of four consecutive jobs:
  - $(10-2) + (20-2) + (30-2) + (40-2) = 92$

$$\mathbb{P}\left[\sum_4 \text{pET} \geq 92\right] = 1$$

- Sum of four pWCETs is insufficient:
  - E.g., $12 + 12 + 12 + 12 = 48$ has nonzero probability

$$\mathbb{P}\left[\sum_4 \text{pWCET} \geq 92\right] < 1$$

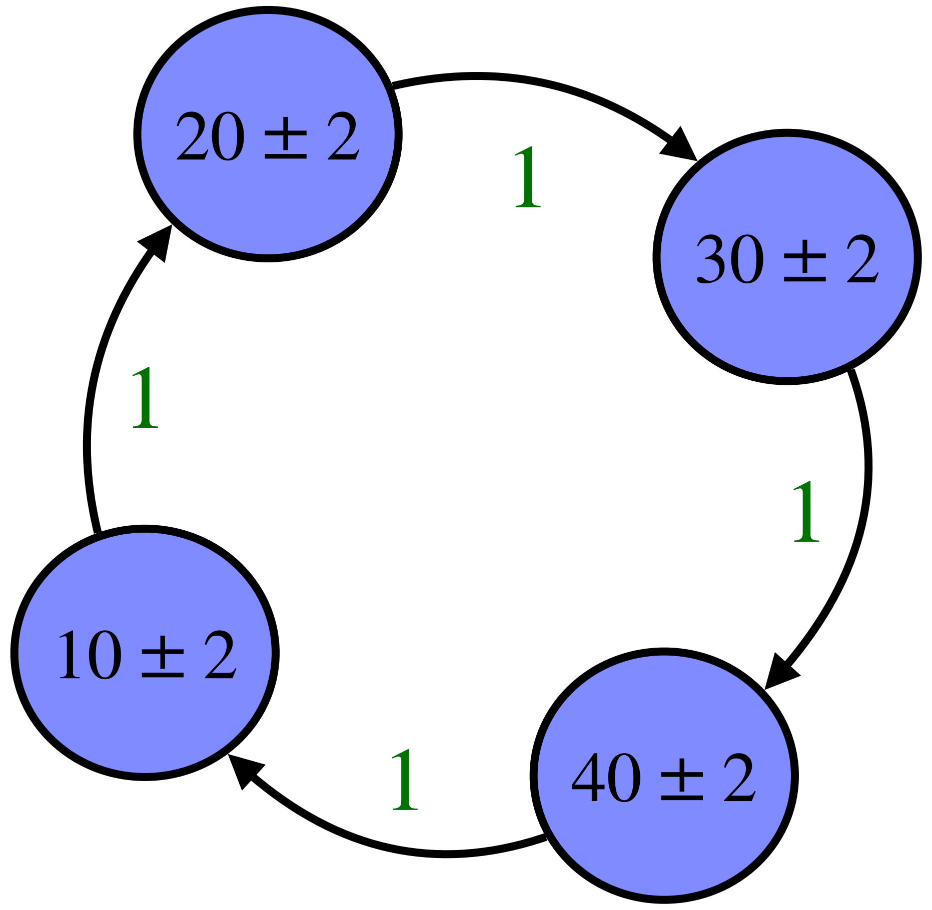
[1] Davis, Robert Ian, and Liliana Cucu-Grosjean. "A survey of probabilistic timing analysis techniques for real-time systems."

SOTA pWCET *DOES NOT* ENABLE IID ANALYSIS

Already noted in [1]

A toy system: [1]

- ➔ Time-predictable hardware
- ➔ System has **four** states
- ➔ State **cycling through** its four possible values
- ➔ Small variability in each of the states
- ➔ Starts with random state



➔ Resulting pET distribution: [1]

$$\begin{pmatrix} 10 \pm 2 & 20 \pm 2 & 30 \pm 2 & 40 \pm 2 \\ 1/4 & 1/4 & 1/4 & 1/4 \end{pmatrix}$$

➔ Valid pWCET distribution: [1]

$$\begin{pmatrix} 12 & 22 & 32 & 42 \\ 1/4 & 1/4 & 1/4 & 1/4 \end{pmatrix}$$

Not "appropriate" for IID-based analysis

Except that ....

- ➔ Smallest workload of four consecutive jobs:
  - ➔ $(10 - 2) + (20 - 2) + (30 - 2) + (40 - 2) = 92$
- ➔ Sum of four pWCETs is insufficient:
  - ➔ E.g., $12 + 12 + 12 + 12 = 48$ has nonzero probability

$$\mathbb{P}\left[\sum_{4} \text{pET} \geq 92\right] = 1$$

$$\mathbb{P}\left[\sum_{4} \text{pWCET} \geq 92\right] < 1$$

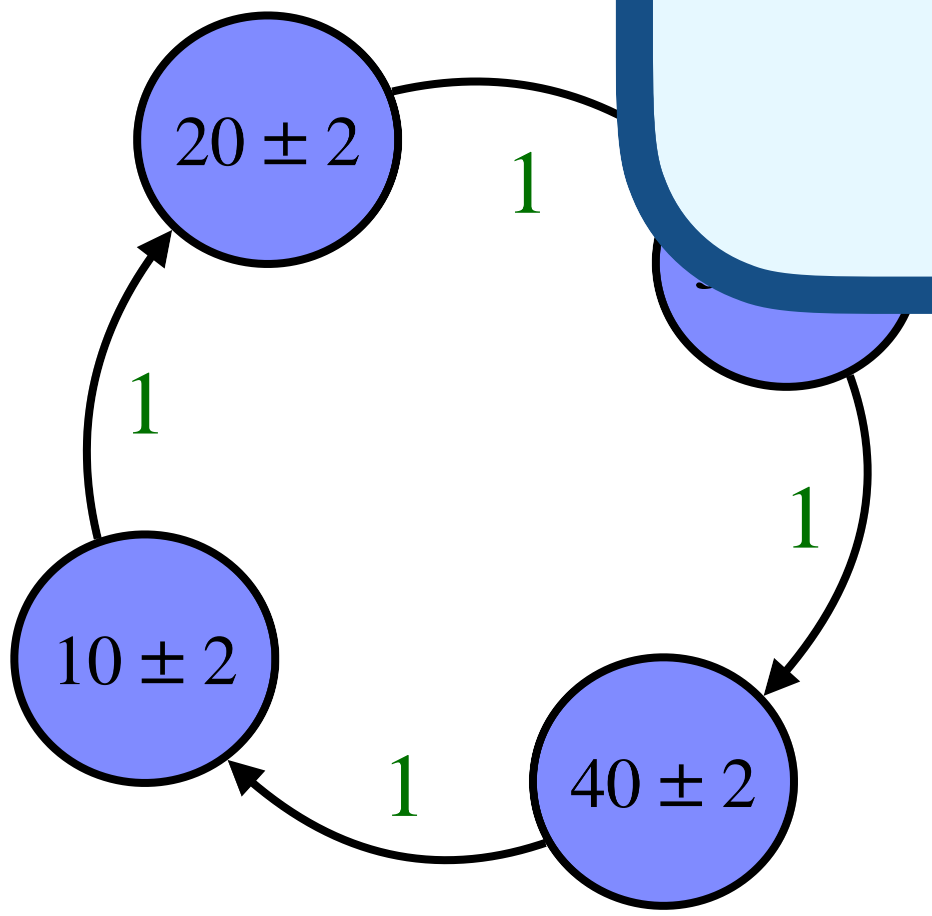
[1] Davis, Robert Ian, and Liliana Cucu-Grosjean. "A survey of probabilistic timing analysis techniques for real-time systems."

SOTA pWCET *DOES NOT* ENABLE IID ANALYSIS

Already noted in [1]

A toy system: [1]

- Time-predictable hardware
- System has **four**
- State **cycling thr**
- Small variability i
- Starts with rando



- Resulting pET distribution: [1]

$$\begin{pmatrix} 10 \pm 2 & 20 \pm 2 & 30 \pm 2 & 40 \pm 2 \\ & & & 1/4 \end{pmatrix}$$

"appropriate" for
-based analysis

So, what is "appropriate" pWCET?

$\mathbb{P}\left[\sum_4 \text{pET} \geq 92\right] = 1$

- $(10-2)+(20-2)+(30-2)+(40-2) = 92$

$\mathbb{P}\left[\sum_4 \text{pWCET} \geq 92\right] < 1$

- Sum of four pWCETs is insufficient:
  - E.g., $12+12+12+12 = 48$ has nonzero probability

[1] Davis, Robert Ian, and Liliana Cucu-Grosjean. "A survey of probabilistic timing analysis techniques for real-time systems."

OUR PROPOSAL:
AXIOMATIC pWCET

DESIGN GOALS

DESIGN GOALS

Formal definitions of pET and pWCET

- *Definitions that are mathematically formal and unambiguous*

ω

DESIGN GOALS

Formal definitions of pET and pWCET

- *Definitions that are mathematically formal and unambiguous*

ω

Adequacy property: pWCET enables IID analysis

- *Any sound analysis assuming IID costs must result in a valid estimation*

$\forall$

DESIGN GOALS

Formal definitions of pET and pWCET

- *Definitions that are mathematically formal and unambiguous*

ω

Adequacy property: pWCET enables IID analysis

- *Any sound analysis assuming IID costs must result in a valid estimation*

$\forall$

Precise enough to be **mechanisable** in Coq

- *pET, pWCET and adequacy property with its proof must be formalisable in Coq proof assistant*

AXIOMATIC pWCET

[1] Davis, Robert Ian, and Liliana Cucu-Grosjean. "A survey of probabilistic schedulability analysis techniques for real-time systems."

▶ **Definition 2.** The *probabilistic Worst-Case Execution Time (pWCET)* distribution for a task is the least upper bound, in the sense of the greater than or equal to operator $\succeq$ (defined below), on the execution time distribution of the jobs of the task for every valid scenario of operation, where a *scenario* of operation is defined as an infinitely repeating sequence of input states (including both input values and software state variables) and initial hardware states that characterise a feasible way in which recurrent execution of the task may occur. [1]

AXIOMATIC pWCET

[1] Davis, Robert Ian, and Liliana Cucu-Grosjean. "A survey of probabilistic schedulability analysis techniques for real-time systems."

▶ **Definition 2.** The *probabilistic Worst-Case Execution Time (pWCET)* distribution for a task is the least upper bound, in the sense of the greater than or equal to operator $\succeq$ (defined below), on the execution time distribution of the jobs of the task for every valid scenario of operation, where a *scenario* of operation is defined as an infinitely repeating sequence of input states (including both input values and software state variables) and initial hardware states that characterise a feasible way in which recurrent execution of the task may occur. [1]

AXIOMATIC pWCET

Def. 7 (🐓).

[1] Davis, Robert Ian, and Liliana Cucu-Grosjean. "A survey of probabilistic schedulability analysis techniques for real-time systems."

▶ **Definition 2.** The *probabilistic Worst-Case Execution Time (pWCET)* distribution for a task is the least upper bound, in the sense of the greater than or equal to operator $\succeq$ (defined below), on the execution time distribution of the jobs of the task for every valid scenario of operation, where a *scenario* of operation is defined as an infinitely repeating sequence of input states (including both input values and software state variables) and initial hardware states that characterise a feasible way in which recurrent execution of the task may occur. [1]

AXIOMATIC pWCET

Def. 7 (🐓). *A monotonically increasing function $F_i : \mathbb{W} \to [0,1]$ with $F_i(0) = 0$ and $\lim_{t\to\infty} F_i(t) = 1$ is an* axiomatic pWCET *for a task τ_i if*

[1] Davis, Robert Ian, and Liliana Cucu-Grosjean. "A survey of probabilistic schedulability analysis techniques for real-time systems."

▶ **Definition 2.** The *probabilistic Worst-Case Execution Time (pWCET)* distribution for a task is the least upper bound, in the sense of the greater than or equal to operator $\succeq$ (defined below), on the execution time distribution of the jobs of the task for every valid scenario of operation, where a *scenario* of operation is defined as an infinitely repeating sequence of input states (including both input values and software state variables) and initial hardware states that characterise a feasible way in which recurrent execution of the task may occur. [1]

AXIOMATIC pWCET

Def. 7 (❦). *A monotonically increasing function $F_i : \mathbb{W} \to [0, 1]$ with $F_i(0) = 0$ and $\lim_{t\to\infty} F_i(t) = 1$ is an axiomatic* pWCET *for a task τ_i if, for every $J \in \tau_i$ and every fixed arrival sequence $\xi \in \Xi$, there exists a partition $\mathfrak{S}$ (Def. 4) such that*

Def. 4 (❦). *A partition $\mathfrak{S} \triangleq \{S_l\}_l$ is any finite, or countably infinite, disjoint cover of all positive-probability elements of Ω.*

[1] Davis, Robert Ian, and Liliana Cucu-Grosjean. "A survey of probabilistic schedulability analysis techniques for real-time systems."

▶ **Definition 2.** The *probabilistic Worst-Case Execution Time (pWCET)* distribution for a task is the least upper bound, in the sense of the greater than or equal to operator $\succeq$ (defined below), on the execution time distribution of the jobs of the task for every valid scenario of operation, where a *scenario* of operation is defined as an infinitely repeating sequence of input states (including both input values and software state variables) and initial hardware states that characterise a feasible way in which recurrent execution of the task may occur. [1]

AXIOMATIC pWCET

Def. 7 (❦). *A monotonically increasing function $F_i : \mathbb{W} \to [0,1]$ with $F_i(0) = 0$ and $\lim_{t\to\infty} F_i(t) = 1$ is an axiomatic pWCET for a task τ_i if, for every $J \in \tau_i$ and every fixed arrival sequence $\xi \in \Xi$, there exists a partition $\mathfrak{S}$ (Def. 4) such that*

2) *F_i $\mathfrak{S}$-dominates $\mathcal{C}_J$ w.r.t. ξ (Def. 6).*

Def. 4 (❦). *A partition $\mathfrak{S} \triangleq \{S_l\}_l$ is any finite, or countably infinite, disjoint cover of all positive-probability elements of Ω.*

Def. 6 (❦). *Given a job $J \in \mathbb{J}$, a fixed arrival sequence ξ, and a partition $\mathfrak{S}$, a function $F : \mathbb{W} \to [0,1]$ $\mathfrak{S}$-dominates $\mathcal{C}_J$ iff*

$$\forall S_l \in \mathfrak{S} \text{ s.th. } \mathbb{P}[S_l \wedge \xi] > 0 : \quad \mathbb{F}[\mathcal{C}_J | S_l \wedge \xi] \preceq F.$$

[1] Davis, Robert Ian, and Liliana Cucu-Grosjean. "A survey of probabilistic schedulability analysis techniques for real-time systems."

▶ **Definition 2.** The *probabilistic Worst-Case Execution Time (pWCET)* distribution for a task is the least upper bound, in the sense of the greater than or equal to operator $\succeq$ (defined below), on the execution time distribution of the jobs of the task for every valid scenario of operation, where a *scenario* of operation is defined as an infinitely repeating sequence of input states (including both input values and software state variables) and initial hardware states that characterise a feasible way in which recurrent execution of the task may occur. [1]

AXIOMATIC pWCET

Def. 7 (❦). *A monotonically increasing function $F_i : \mathbb{W} \to [0,1]$ with $F_i(0) = 0$ and $\lim_{t\to\infty} F_i(t) = 1$* is an axiomatic pWCET *for a task τ_i if, for every $J \in \tau_i$ and every fixed arrival sequence $\xi \in \Xi$, there exists a partition $\mathfrak{S}$ (Def. 4) such that*

1) *$\mathcal{C}_J$ is partition-independent w.r.t. ξ and $\mathfrak{S}$ (Def. 5)*, and
2) *F_i $\mathfrak{S}$-dominates $\mathcal{C}_J$ w.r.t. ξ (Def. 6).*

Def. 4 (❦). *A partition $\mathfrak{S} \triangleq \{S_l\}_l$ is any finite, or countably infinite, disjoint cover of all positive-probability elements of Ω.*

Def. 6 (❦). *Given a job $J \in \mathbb{J}$, a fixed arrival sequence ξ, and a partition $\mathfrak{S}$, a function $F : \mathbb{W} \to [0,1]$ $\mathfrak{S}$-dominates $\mathcal{C}_J$ iff*

$$\forall S_l \in \mathfrak{S} \text{ s.th. } \mathbb{P}[S_l \wedge \xi] > 0 : \quad \mathbb{F}[\mathcal{C}_J | S_l \wedge \xi] \preceq F.$$

Def. 5 (❦). *Given a job $J \in \mathbb{J}$, a fixed arrival sequence ξ, and a partition $\mathfrak{S}$, job J's pET is* partition-independent w.r.t. $\mathfrak{S}$ *iff, for any set $G \subseteq \mathbb{J}$ with $J \notin G$ and any fixed cost vector $\vec{c}_\bullet$:*

$$\forall S_l \in \mathfrak{S} \text{ s.th. } \mathbb{P}[S_l \wedge \xi] > 0 :$$
$$\mathbb{P}\left[\mathcal{C}_J = \vec{c}_J \wedge \forall J' \in G : \mathcal{C}_{J'} = \vec{c}_{J'} | S_l \wedge \xi\right]$$
$$= \mathbb{P}\left[\mathcal{C}_J = \vec{c}_J | S_l \wedge \xi\right] \cdot \mathbb{P}\left[\forall J' \in G : \mathcal{C}_{J'} = \vec{c}_{J'} | S_l \wedge \xi\right].$$

[1] Davis, Robert Ian, and Liliana Cucu-Grosjean. "A survey of probabilistic schedulability analysis techniques for real-time systems."

▶ **Definition 2.** The *probabilistic Worst-Case Execution Time (pWCET)* distribution for a task is the least upper bound, in the sense of the greater than or equal to operator $\succeq$ (defined below), on the execution time distribution of the jobs of the task for every valid scenario of operation, where a *scenario* of operation is defined as an infinitely repeating sequence of input states (including both input values and software state variables) and initial hardware states that characterise a feasible way in which recurrent execution of the task may occur. [1]

AXIOMATIC pWCET

Def. 7 (🐓). *A monotonically increasing function $F_i \colon \mathbb{W} \to [0,1]$ with $F_i(0) = 0$ and $\lim_{t\to\infty} F_i(t) = 1$ is an axiomatic pWCET for a task τ_i if, for every $J \in \tau_i$ and every fixed arrival sequence $\xi \in \Xi$, there exists a partition $\mathfrak{S}$ (Def. 4) such that*

1) *$\mathcal{C}_J$ is partition-independent w.r.t. ξ and $\mathfrak{S}$ (Def. 5), and*
2) *F_i $\mathfrak{S}$-dominates $\mathcal{C}_J$ w.r.t. ξ (Def. 6).*

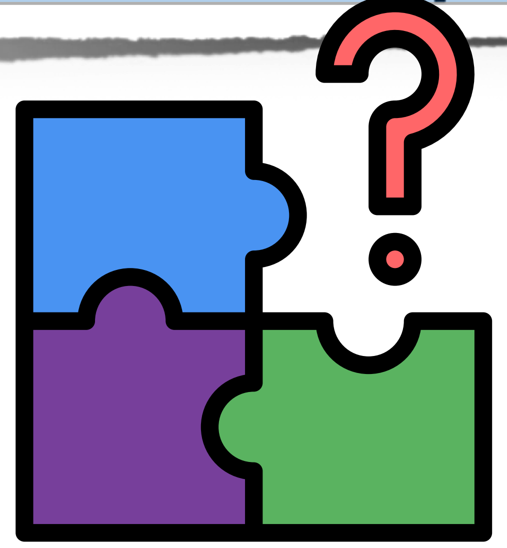
Def. 4 (🐓). *A partition $\mathfrak{S} \triangleq \{S_l\}_l$ is any finite, or countably infinite, disjoint cover of all positive-probability elements of Ω.*

Def. 6 (🐓). *Given a job $J \in \mathbb{J}$, a fixed arrival sequence ξ, and a partition $\mathfrak{S}$, a function $F \colon \mathbb{W} \to [0,1]$ $\mathfrak{S}$-dominates $\mathcal{C}_J$ iff*

$$\forall S_l \in \mathfrak{S} \text{ s.th. } \mathbb{P}[S_l \wedge \xi] > 0 \colon \quad \mathbb{F}[\mathcal{C}_J | S_l \wedge \xi] \preceq F.$$

Def. 5 (🐓). *Given a job $J \in \mathbb{J}$, a fixed arrival sequence ξ, and a partition $\mathfrak{S}$, job J's pET is* partition-independent w.r.t. *$\mathfrak{S}$ iff, for any set $G \subseteq \mathbb{J}$ with $J \notin G$ and any fixed cost vector $\vec{c}_\bullet$:*

$$\forall S_l \in \mathfrak{S} \text{ s.th. } \mathbb{P}[S_l \wedge \xi] > 0 \colon$$
$$\mathbb{P}\left[\mathcal{C}_J = \vec{c}_J \wedge \forall J' \in G \colon \mathcal{C}_{J'} = \vec{c}_{J'} | S_l \wedge \xi\right]$$
$$= \mathbb{P}\left[\mathcal{C}_J = \vec{c}_J | S_l \wedge \xi\right] \cdot \mathbb{P}\left[\forall J' \in G \colon \mathcal{C}_{J'} = \vec{c}_{J'} | S_l \wedge \xi\right].$$



"Appropriate" pWCET part?

[1] Davis, Robert Ian, and Liliana Cucu-Grosjean. "A survey of probabilistic schedulability analysis techniques for real-time systems."

▶ **Definition 2.** The *probabilistic Worst-Case Execution Time (pWCET)* distribution for a task is the least upper bound, in the sense of the greater than or equal to operator $\succeq$ (defined below), on the execution time distribution of the jobs of the task for every valid scenario of operation, where a *scenario* of operation is defined as an infinitely repeating sequence of input states (including both input values and software state variables) and initial hardware states that characterise a feasible way in which recurrent execution of the task may occur. [1]

AXIOMATIC pWCET

Def. 7 (🐓). *A monotonically increasing function $F_i : \mathbb{W} \to [0,1]$ with $F_i(0) = 0$ and $\lim_{t\to\infty} F_i(t) = 1$ is an axiomatic pWCET for a task τ_i if, for every $J \in \tau_i$ and every fixed arrival sequence $\xi \in \Xi$, there exists a partition $\mathfrak{S}$ (Def. 4) such that*

1) *$\mathcal{C}_J$ is partition-independent w.r.t. ξ and $\mathfrak{S}$ (Def. 5), and*
2) *F_i $\mathfrak{S}$-dominates $\mathcal{C}_J$ w.r.t. ξ (Def. 6).*

Def. 4 (🐓). *A partition $\mathfrak{S} \triangleq \{S_l\}_l$ is any finite, or countably infinite, disjoint cover of all positive-probability elements of Ω.*

Def. 6 (🐓). *Given a job $J \in \mathbb{J}$, a fixed arrival sequence ξ, and a partition $\mathfrak{S}$, a function $F : \mathbb{W} \to [0,1]$ $\mathfrak{S}$-dominates $\mathcal{C}_J$ iff*

$$\forall S_l \in \mathfrak{S} \text{ s.th. } \mathbb{P}[S_l \wedge \xi] > 0: \quad \mathbb{F}[\mathcal{C}_J | S_l \wedge \xi] \preceq F.$$

Def. 5 (🐓). *Given a job $J \in \mathbb{J}$, a fixed arrival sequence ξ, and a partition $\mathfrak{S}$, job J's pET is* partition-independent w.r.t. $\mathfrak{S}$ *iff, for any set $G \subseteq \mathbb{J}$ with $J \notin G$ and any fixed cost vector $\vec{c}_\bullet$:*

$$\forall S_l \in \mathfrak{S} \text{ s.th. } \mathbb{P}[S_l \wedge \xi] > 0:$$
$$\mathbb{P}\left[\mathcal{C}_J = \vec{c}_J \wedge \forall J' \in G : \mathcal{C}_{J'} = \vec{c}_{J'} | S_l \wedge \xi\right]$$
$$= \mathbb{P}\left[\mathcal{C}_J = \vec{c}_J | S_l \wedge \xi\right] \cdot \mathbb{P}\left[\forall J' \in G : \mathcal{C}_{J'} = \vec{c}_{J'} | S_l \wedge \xi\right].$$

Axiomatic pWCET: *scenario of operation* must ensure that jobs' pETs become independent

[1] Davis, Robert Ian, and Liliana Cucu-Grosjean. "A survey of probabilistic schedulability analysis techniques for real-time systems."

ADEQUACY

ADEQUACY: FORMAL BASIS FOR IID REASONING

How do we know that an IID-based analysis that uses axiomatic pWCET will obtain a sound bound?

ADEQUACY: FORMAL BASIS FOR IID REASONING

Probabilistic Response Time (pRT)

How do we know that an IID-based analysis that uses axiomatic pWCET will obtain a sound bound?

Intuitively, we want to prove:

➔ Ground-truth pRT is $\preceq$-bounded by pRT derived via pWCETs

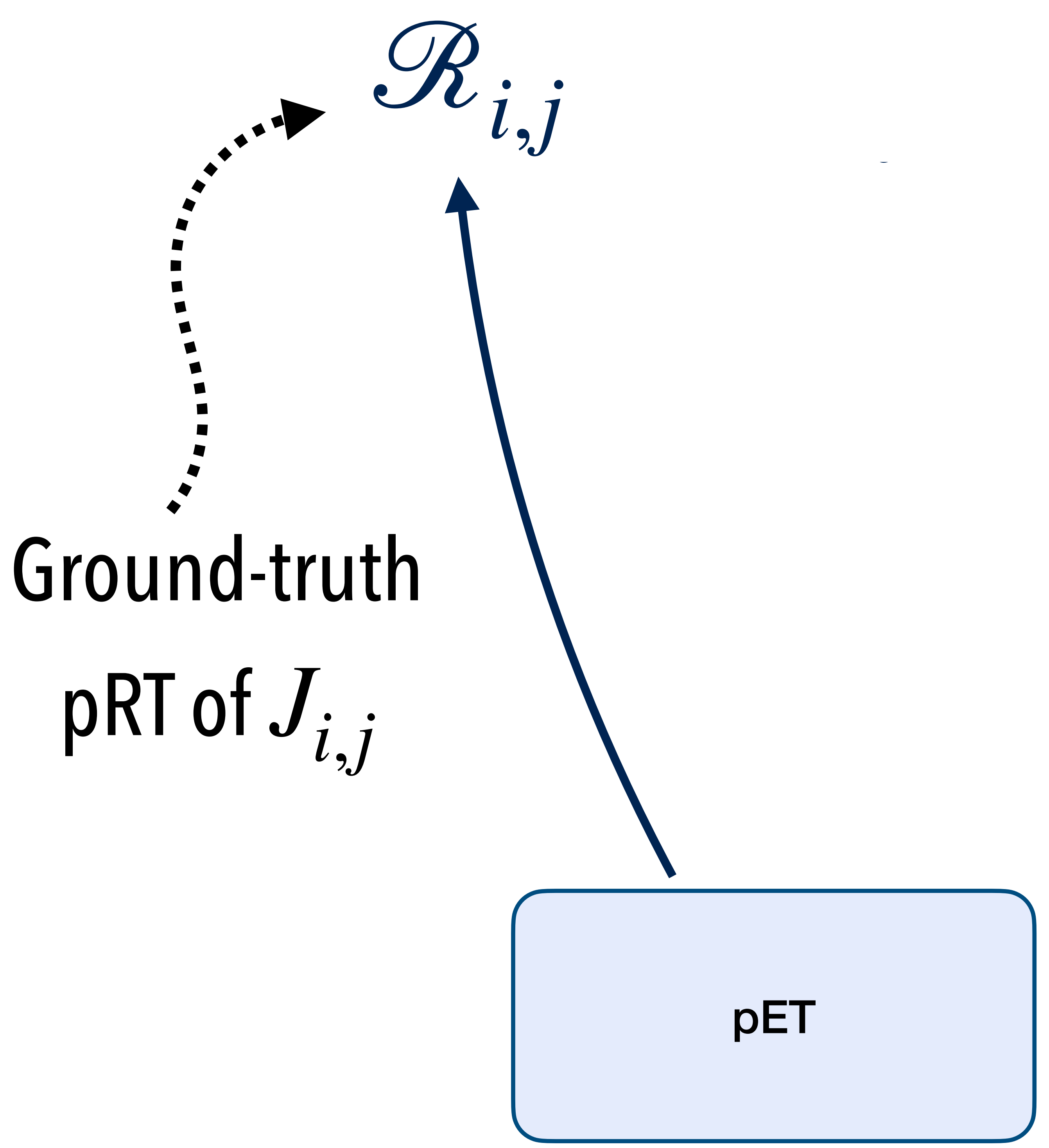
ADEQUACY: FORMAL BASIS FOR IID REASONING

Probabilistic Response Time (pRT)

How do we know that an IID-based analysis that uses axiomatic pWCET will obtain a sound bound?

Intuitively, we want to prove:

➔ Ground-truth pRT is $\preceq$-bounded by pRT derived via pWCETs



ADEQUACY: FORMAL BASIS FOR IID REASONING

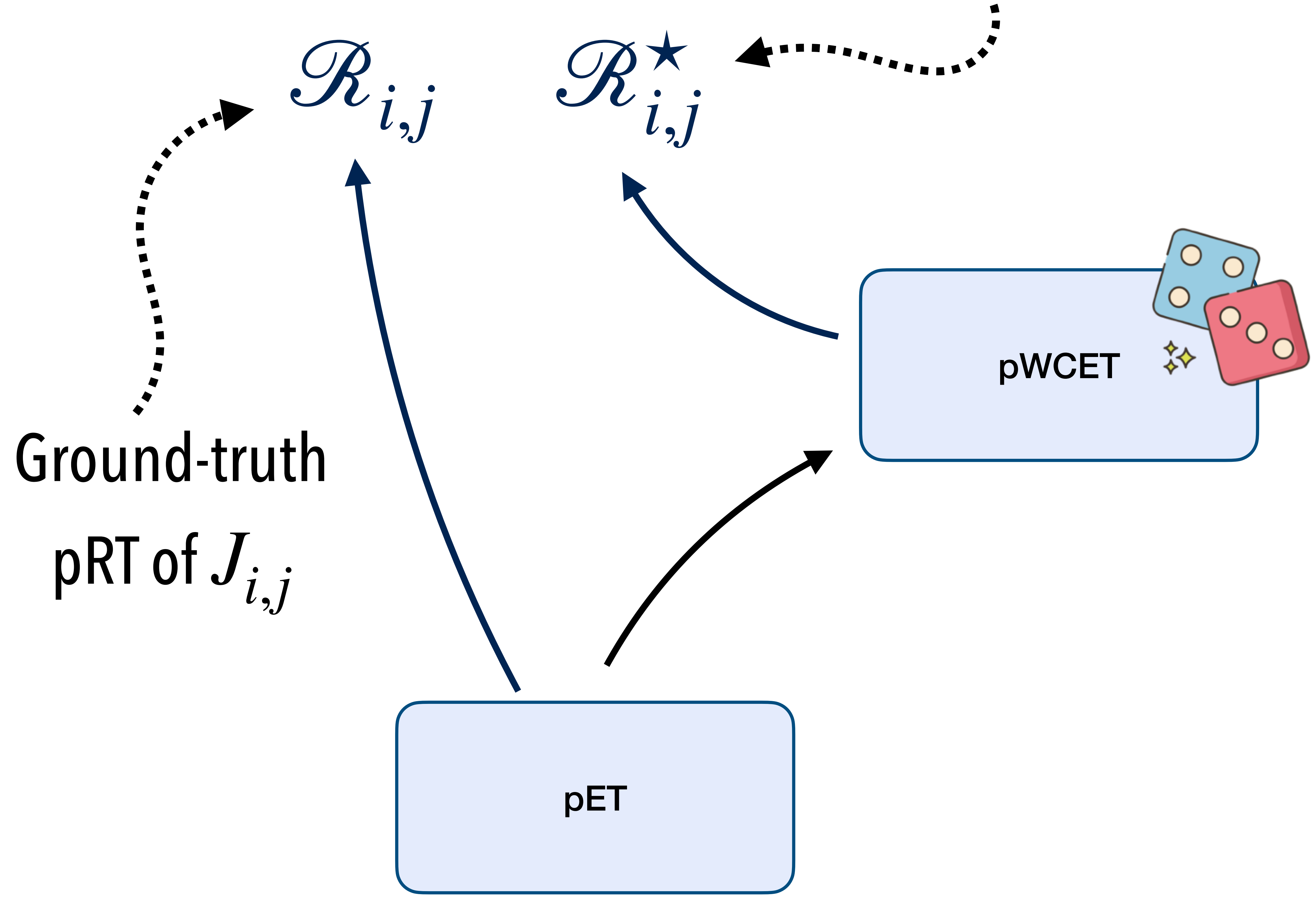
Probabilistic Response Time (pRT)

How do we know that an IID-based analysis that uses axiomatic pWCET will obtain a sound bound?

pRT of $J_{i,j}$ obtained by **any valid IID-based analysis** using axiomatic pWCET

Intuitively, we want to prove:

➔ Ground-truth pRT is ⪯-bounded by pRT derived via pWCETs



ADEQUACY: FORMAL BASIS FOR IID REASONING

Probabilistic Response Time (pRT)

How do we know that an IID-based analysis that uses axiomatic pWCET will obtain a sound bound?

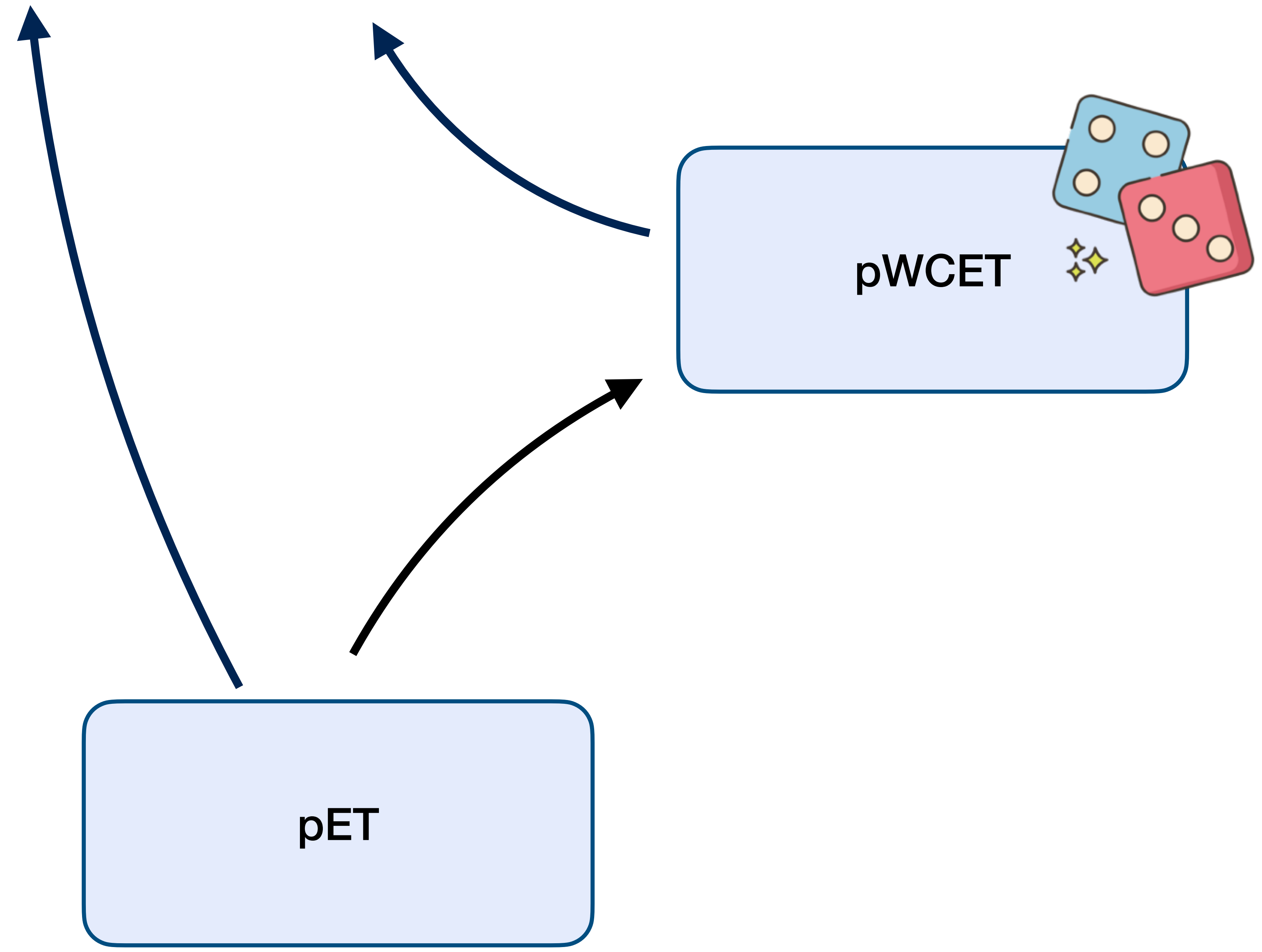
pRT of $J_{i,j}$ obtained by **any valid IID-based analysis** using axiomatic pWCET

Intuitively, we want to prove:

➔ Ground-truth pRT is $\preceq$-bounded by pRT derived via pWCETs

$$\mathcal{R}_{i,j} \preceq \mathcal{R}^{\star}_{i,j}$$

Ground-truth pRT of $J_{i,j}$



ADEQUACY: FORMAL BASIS FOR IID REASONING

How do we know that an IID-based analysis that uses axiomatic pWCET will obtain a sound bound?

Probabilistic Response Time (pRT)

Intuitively, we want to prove:

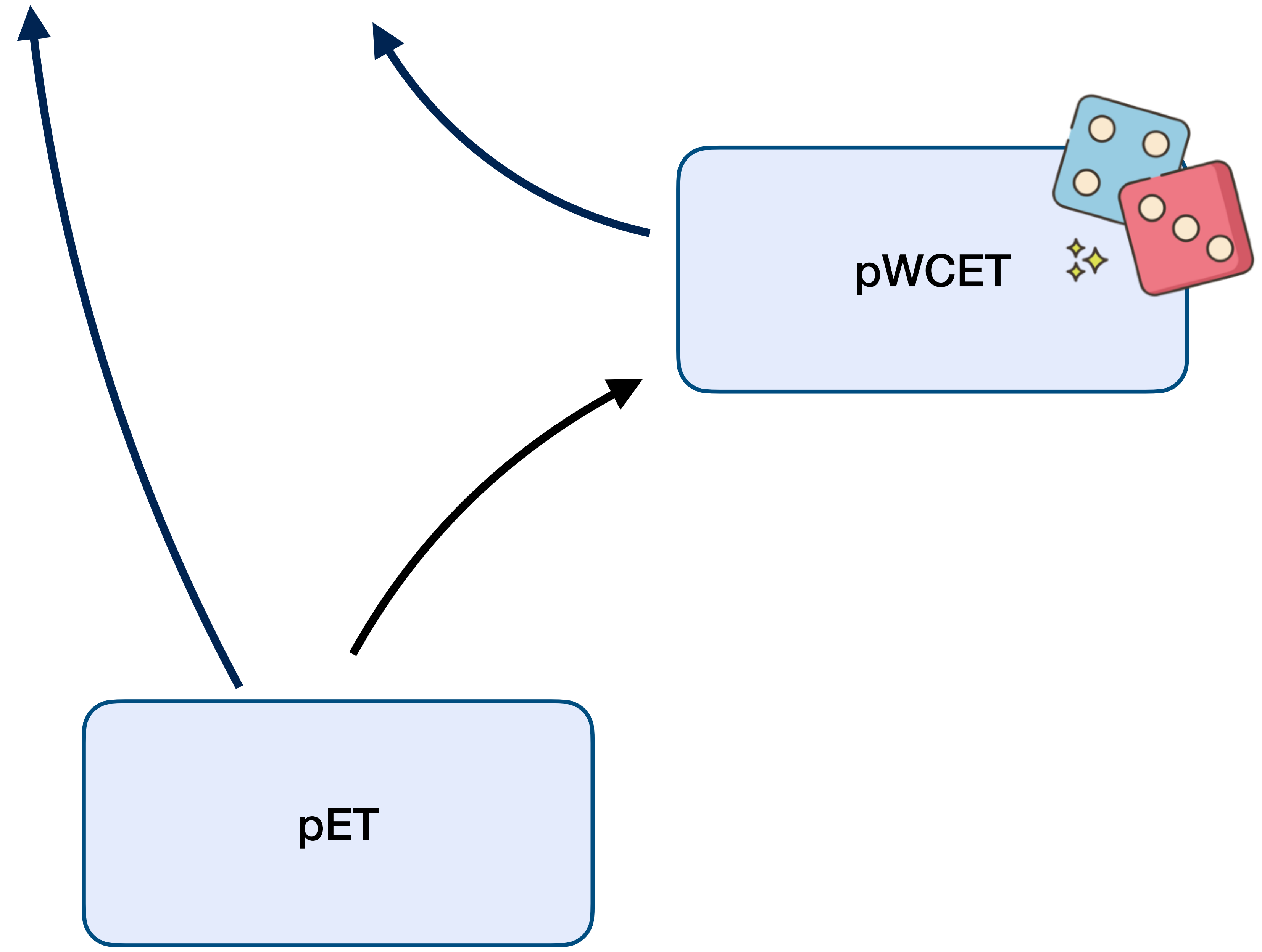
➔ Ground-truth pRT is $\preceq$-bounded by pRT derived via pWCETs

Formal statement is **surprisingly** tricky and involves the notion of "replacement" of pETs with pWCETs

pRT of $J_{i,j}$ obtained by **any valid IID-based analysis** using axiomatic pWCET

$$\mathscr{R}_{i,j} \preceq \mathscr{R}^{\star}_{i,j}$$

Ground-truth pRT of $J_{i,j}$



AXIOMATIC pWCET IS ADEQUATE

Theorem *(paraphrased)*. Consider a job $J_{i,j}$. Let $\mathscr{R}_{i,j}$ be the pRT of $J_{i,j}$ in the initial system and $\mathscr{R}^{\star}_{i,j}$ be the pRT of $J_{i,j}$ in a simplified system obtained via pWCET F_i. Then $\mathscr{R}_{i,j} \preceq \mathscr{R}^{\star}_{i,j}$.

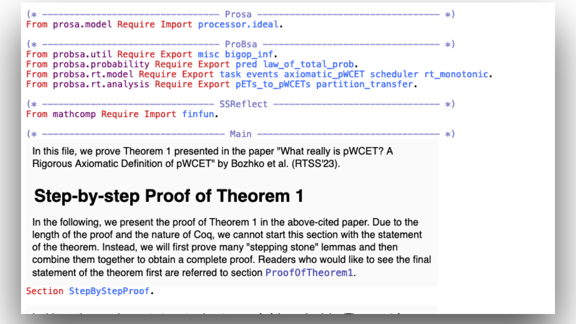
AXIOMATIC pWCET IS ADEQUATE

Theorem *(paraphrased)*. Consider a job $J_{i,j}$. Let $\mathscr{R}_{i,j}$ be the pRT of $J_{i,j}$ in the initial system and $\mathscr{R}^{\star}_{i,j}$ be the pRT of $J_{i,j}$ in a simplified system obtained via pWCET F_i. Then $\mathscr{R}_{i,j} \preceq \mathscr{R}^{\star}_{i,j}$.

Hint:

1. Use axiomatic pWCET to construct a "copy" of the initial system, where pETs are replaced with job costs that are, **by construction**, IID and have distribution F_i
2. Prove that pRT $\mathscr{R}^{\star}_{i,j}$ in the simplified system stochastically dominates the original pRT $\mathscr{R}_{i,j}$

AXIOMATIC pWCET IS ADEQUATE



Theorem *(paraphrased)*. Consider a job $J_{i,j}$. Let $\mathscr{R}_{i,j}$ be the pRT of $J_{i,j}$ in the initial system and $\mathscr{R}^{\star}_{i,j}$ be the pRT of $J_{i,j}$ in a simplified system obtained via pWCET F_i. Then $\mathscr{R}_{i,j} \preceq \mathscr{R}^{\star}_{i,j}$.

Hint:

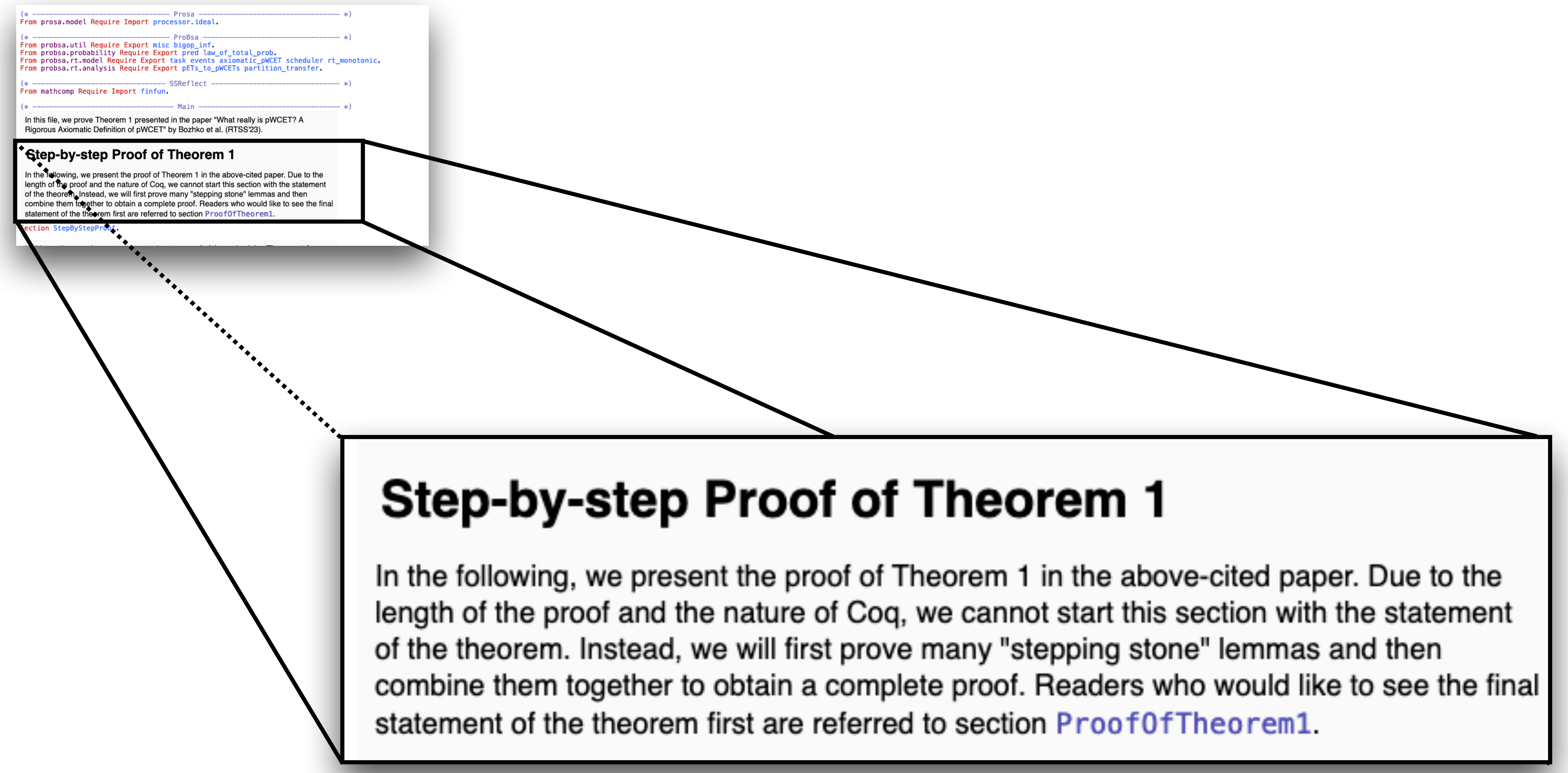
1. Use axiomatic pWCET to construct a "copy" of the initial system, where pETs are replaced with job costs that are, **by construction**, IID and have distribution F_i
2. Prove that pRT $\mathscr{R}^{\star}_{i,j}$ in the simplified system stochastically dominates the original pRT $\mathscr{R}_{i,j}$

AXIOMATIC pWCET IS ADEQUATE

Theorem *(paraphrased)*. Consider a job $J_{i,j}$. Let $\mathscr{R}_{i,j}$ be the pRT of $J_{i,j}$ in the initial system and $\mathscr{R}^{\star}_{i,j}$ be the pRT of $J_{i,j}$ in a simplified system obtained via pWCET F_i. Then $\mathscr{R}_{i,j} \preceq \mathscr{R}^{\star}_{i,j}$.

Hint:

1. Use axiomatic pWCET to construct a "copy" of the initial system, where pETs are replaced with job costs that are, **by construction**, IID and have distribution F_i
2. Prove that pRT $\mathscr{R}^{\star}_{i,j}$ in the simplified system stochastically dominates the original pRT $\mathscr{R}_{i,j}$

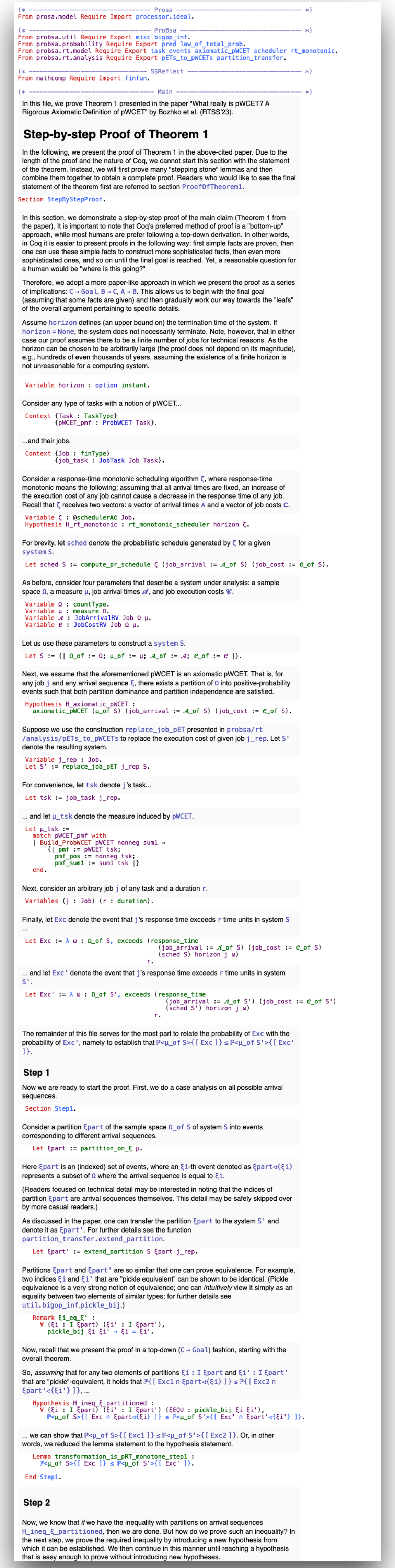


AXIOMATIC pWCET IS ADEQUATE

Theorem *(paraphrased)*. Consider a job $J_{i,j}$. Let $\mathscr{R}_{i,j}$ be the pRT of $J_{i,j}$ in the initial system and $\mathscr{R}^{\star}_{i,j}$ be the pRT of $J_{i,j}$ in a simplified system obtained via pWCET F_i. Then $\mathscr{R}_{i,j} \preceq \mathscr{R}^{\star}_{i,j}$.

Hint:

1. Use axiomatic pWCET to construct a "copy" of the initial system, where pETs are replaced with job costs that are, **by construction**, IID and have distribution F_i
2. Prove that pRT $\mathscr{R}^{\star}_{i,j}$ in the simplified system stochastically dominates the original pRT $\mathscr{R}_{i,j}$



AXIOMATIC pWCET IS ADEQUATE

Theorem *(paraphrased)*. Consider a job $J_{i,j}$. Let $\mathscr{R}_{i,j}$ be the pRT of $J_{i,j}$ in the initial system and $\mathscr{R}^{\star}_{i,j}$ be the pRT of $J_{i,j}$ in a simplified system obtained via pWCET F_i. Then $\mathscr{R}_{i,j} \preceq \mathscr{R}^{\star}_{i,j}$.

Hint:

1. Use axiomatic pWCET to construct a "copy" of the initial system, where pETs are replaced with job costs that are, **by construction**, IID and have distribution F_i
2. Prove that pRT $\mathscr{R}^{\star}_{i,j}$ in the simplified system stochastically dominates the original pRT $\mathscr{R}_{i,j}$


Step-by-step Proof of Theorem 1

Step 1

Step 2

Step 3

Step 4

Step 5

AXIOMATIC pWCET IS ADEQUATE

Theorem *(paraphrased)*. Consider a job $J_{i,j}$. Let $\mathscr{R}_{i,j}$ be the pRT of $J_{i,j}$ in the initial system and $\mathscr{R}^\star_{i,j}$ be the pRT of $J_{i,j}$ in a simplified system obtained via pWCET F_i. Then $\mathscr{R}_{i,j} \preceq \mathscr{R}^\star_{i,j}$.

Hint:

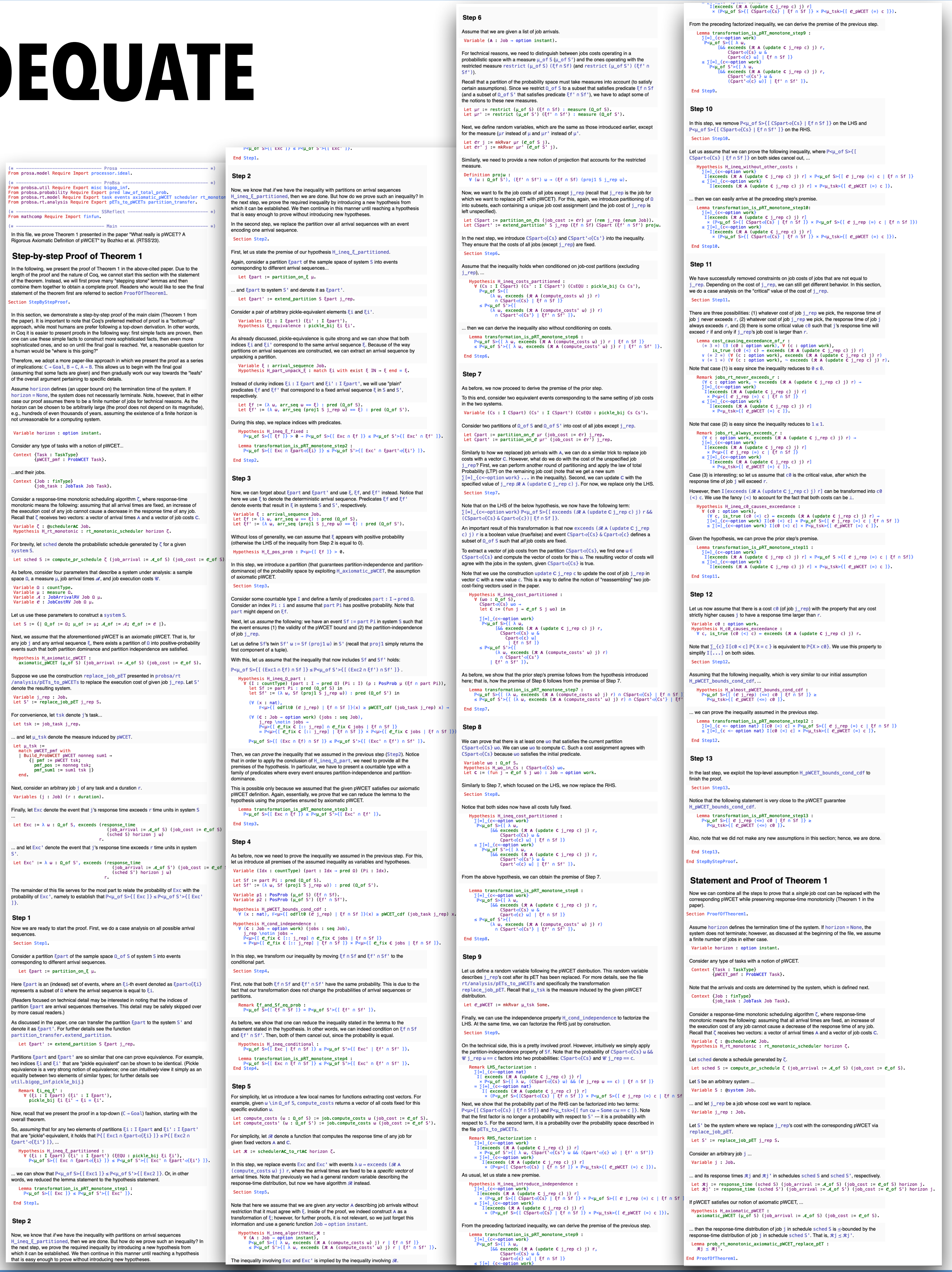
1. Use axiomatic pWCET to construct a "copy" of the initial system, where pETs are replaced with job costs that are, **by construction**, IID and have distribution F_i
2. Prove that pRT $\mathscr{R}^\star_{i,j}$ in the simplified system stochastically dominates the original pRT $\mathscr{R}_{i,j}$

AXIOMATIC pWCET IS ADEQUATE

Theorem *(paraphrased)*. Consider a job $J_{i,j}$. Let $\mathscr{R}_{i,j}$ be the pRT of $J_{i,j}$ in the initial system and $\mathscr{R}^{\star}_{i,j}$ be the pRT of $J_{i,j}$ in a simplified system obtained via pWCET F_i. Then $\mathscr{R}_{i,j} \preceq \mathscr{R}^{\star}_{i,j}$.

Hint:

1. Use axiomatic pWCET to construct a "copy" of the initial system, where pETs are replaced with job costs that are, **by construction**, IID and have distribution F_i
2. Prove that pRT $\mathscr{R}^{\star}_{i,j}$ in the simplified system stochastically dominates the original pRT $\mathscr{R}_{i,j}$



AXIOMATIC pWCET IS ADEQUATE

Theorem *(paraphrased)*. Consider a job $J_{i,j}$. Let $\mathcal{R}_{i,j}$ be the pRT of $J_{i,j}$ in the initial system and $\mathcal{R}^{\star}_{i,j}$ be the pRT of $J_{i,j}$ in a simplified system obtained via pWCET F_i. Then $\mathcal{R}_{i,j} \preceq \mathcal{R}^{\star}_{i,j}$.

Hint:

1. Use axiomatic pWCET to construct a "copy" of the initial system, where pETs are replaced with job costs that are

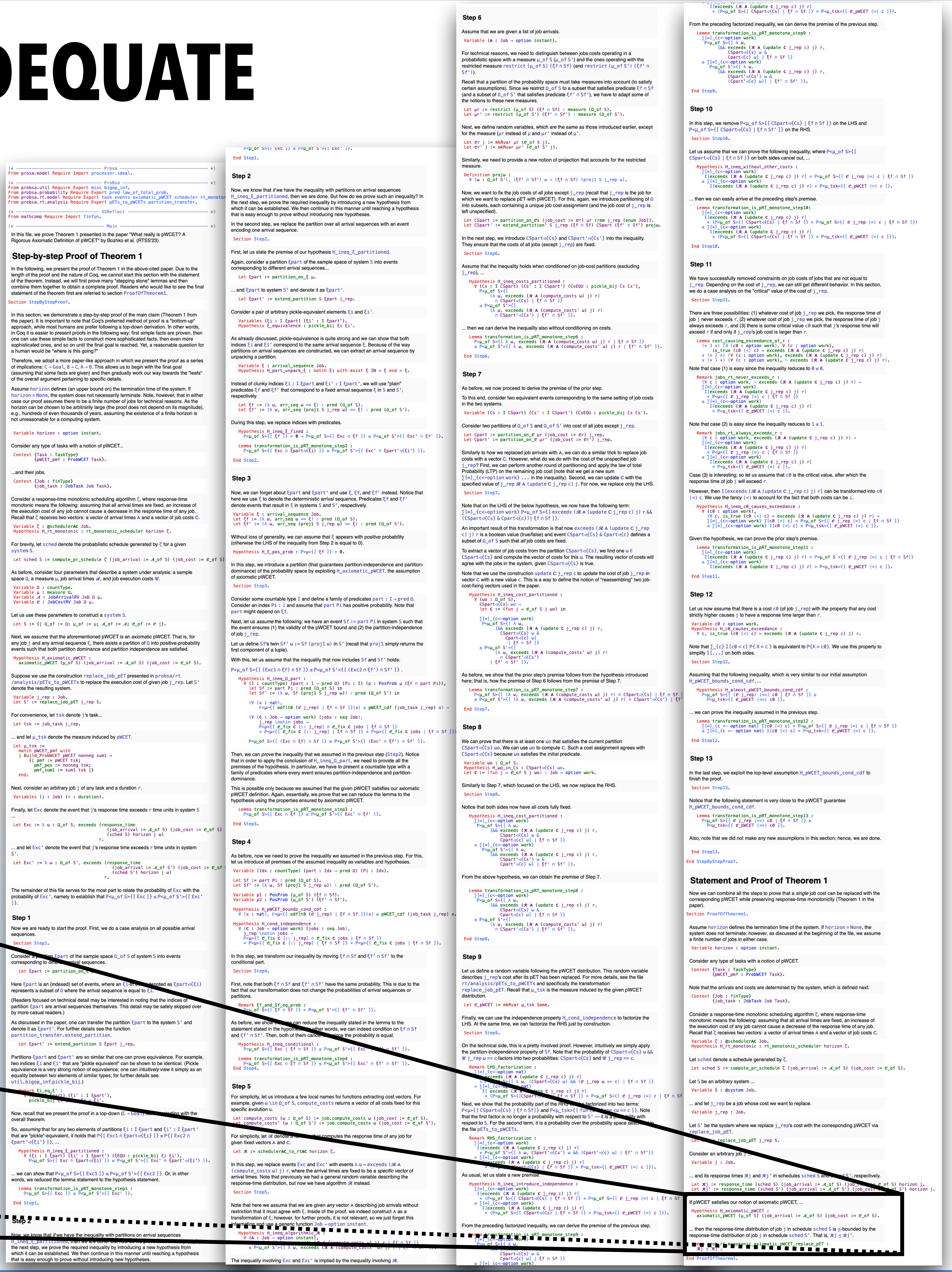
13 steps later ...

If pWCET satisfies our notion of axiomatic pWCET, ...

```
Hypothesis H_axiomatic_pWCET :
  axiomatic_pWCET (μ_of S) (job_arrival := 𝒜_of S) (job_cost := 𝒞_of S).
```

... then the response-time distribution of job j in schedule sched S is ≼-bounded by the response-time distribution of job j in schedule sched S'. That is, ℛj ≼ ℛj'.

```
Lemma prob_rt_monotonic_axiomatic_pWCET_replace_pET :
  ℛj ≼ ℛj'.
```



FORMAL SPECIFICATION AND PROOFS

Clickable links to Coq specification

➔ Each definition, lemma, and proof step is accompanied by a link to the corresponding Coq specification

The LHS and RHS of the inequality can be simplified to $\mathbb{P}[\mathcal{C}_{J_o} > c_0 | \xi \wedge S_l]$ and $\mathbb{P}_f[\widehat{\mathcal{C}}_{J_o} > c_0]$, respectively. Using the fact that $\mathbb{P}[a > b] \leq \mathbb{P}[c > d] \iff \mathbb{P}[a \leq b] \geq \mathbb{P}[c \leq d]$, we transform the inequality to obtain ( ):

$$\mathbb{P}[\mathcal{C}_{J_o} \leq c_0 | \xi \wedge S_l] \geq \mathbb{P}_f[\widehat{\mathcal{C}}_{J_o} \leq c_0].$$

Finally, by construction (Def. 10), $\mathbb{P}_f[\widehat{\mathcal{C}}_{J_o} \leq c_0] = F_i(c_0)$. Hence, we end up with $\mathbb{P}[\mathcal{C}_{J_o} \leq c_0 | \xi \wedge S_l] \geq F_i(c_0)$, which follows ( ) from partition-dominance (Def. 6). □

Step 13

In the last step, we exploit the top-level assumption `H_pWCET_bounds_cond_cdf` to finish the proof.

```
Section Step13.
```

Notice that the following statement is very close to the pWCET guarantee `H_pWCET_bounds_cond_cdf`.

```
  Lemma transformation_is_pRT_monotone_step13 :
    ℙ<μ_of S>{[ 𝓬 j_rep ⟨<=⟩ c0 | ξf ∩ Sf ]} ≥
      ℙ<μ_tsk>{[ 𝓬_pWCET ⟨<=⟩ c0 ]}.
```

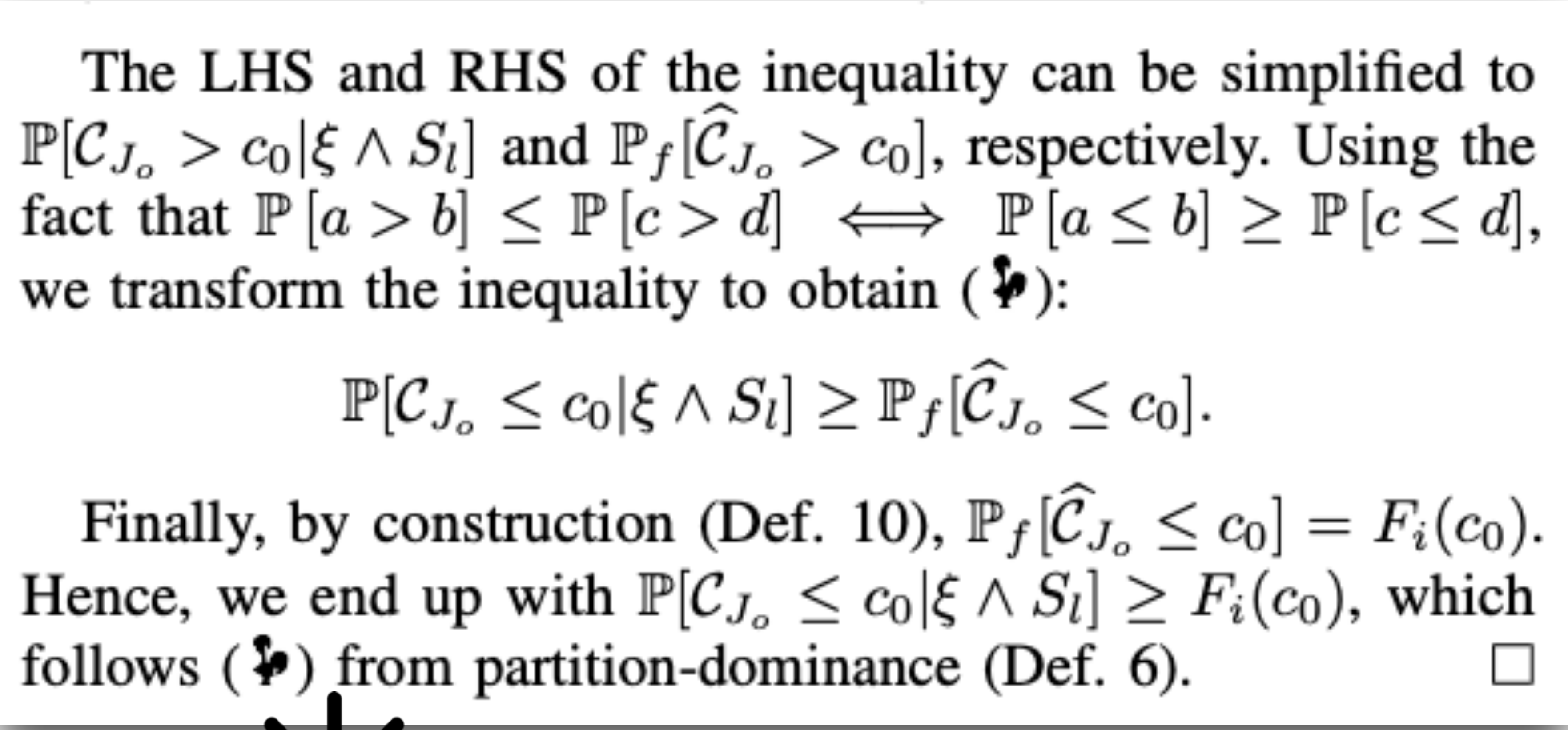
Also, note that we did not make any new assumptions in this section; hence, we are done.

```
End Step13.
```

FORMAL SPECIFICATION AND PROOFS

Clickable links to Coq specification

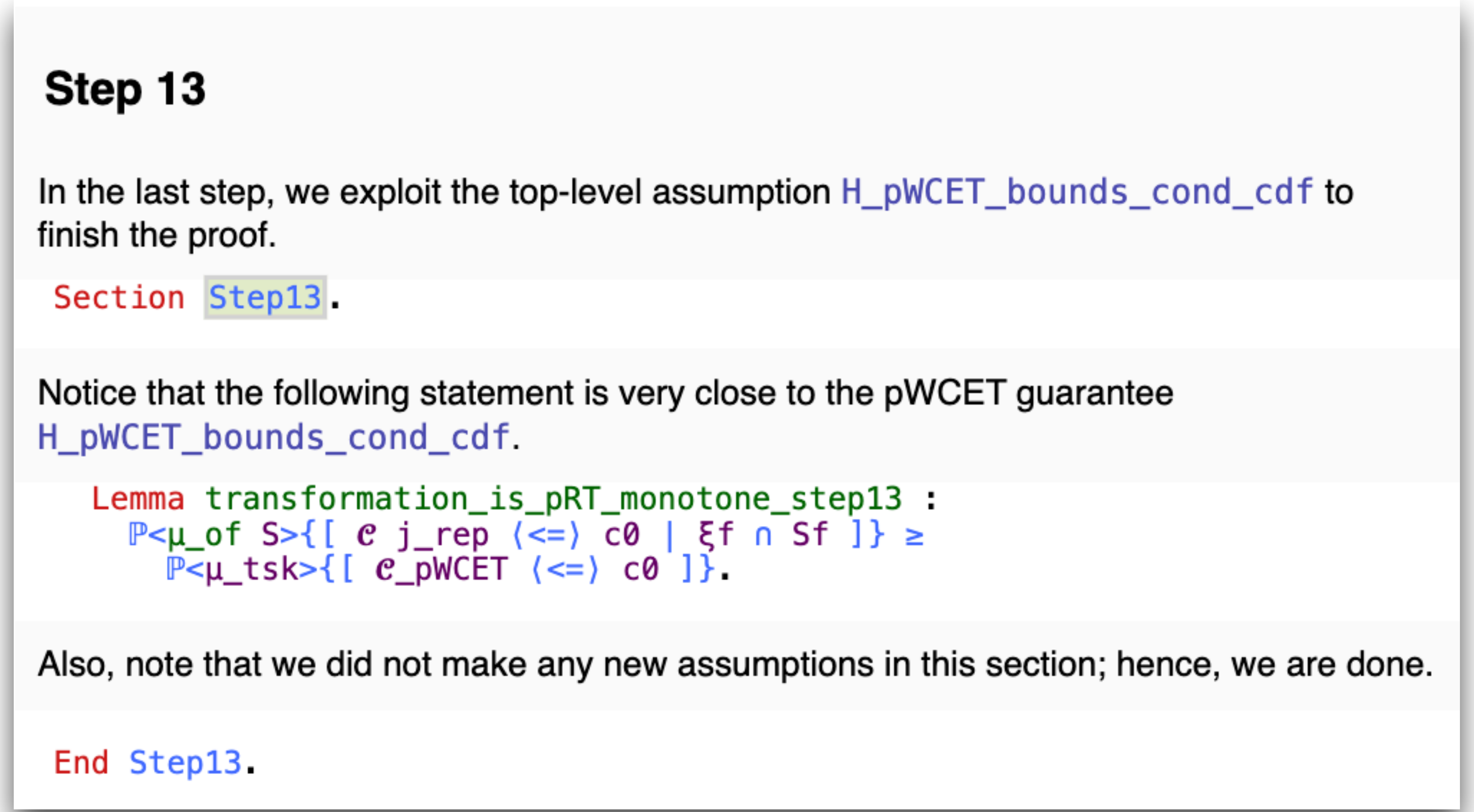
- ➔ Each definition, lemma, and proof step is accompanied by a link to the corresponding Coq specification
- ➔ Links are cumbersome and not clickable in the official IEEE version
- ➔ Links are directly clickable in the version provided on the author websites



The LHS and RHS of the inequality can be simplified to $\mathbb{P}[\mathcal{C}_{J_o} > c_0 | \xi \wedge S_l]$ and $\mathbb{P}_f[\widehat{\mathcal{C}}_{J_o} > c_0]$, respectively. Using the fact that $\mathbb{P}[a > b] \leq \mathbb{P}[c > d] \iff \mathbb{P}[a \leq b] \geq \mathbb{P}[c \leq d]$, we transform the inequality to obtain (♣):

$$\mathbb{P}[\mathcal{C}_{J_o} \leq c_0 | \xi \wedge S_l] \geq \mathbb{P}_f[\widehat{\mathcal{C}}_{J_o} \leq c_0].$$

Finally, by construction (Def. 10), $\mathbb{P}_f[\widehat{\mathcal{C}}_{J_o} \leq c_0] = F_i(c_0)$. Hence, we end up with $\mathbb{P}[\mathcal{C}_{J_o} \leq c_0 | \xi \wedge S_l] \geq F_i(c_0)$, which follows (♣) from partition-dominance (Def. 6). □



Step 13

In the last step, we exploit the top-level assumption H_pWCET_bounds_cond_cdf to finish the proof.

```
Section Step13.
```

Notice that the following statement is very close to the pWCET guarantee H_pWCET_bounds_cond_cdf.

```
  Lemma transformation_is_pRT_monotone_step13 :
    ℙ<μ_of S>{[ 𝓬 j_rep ⟨<=⟩ c0 | ξf ∩ Sf ]} ≥
      ℙ<μ_tsk>{[ 𝓬_pWCET ⟨<=⟩ c0 ]}.
```

Also, note that we did not make any new assumptions in this section; hence, we are done.

```
End Step13.
```

CONCLUSION

CONCLUSION AND FUTURE WORK

What we did:

- ➔ First **fully formal** definitions of pET and pWCET
- ➔ **Adequacy property**: formalization of "safe IID upper bound on pET"
- ➔ **Prove** that our pWCET proposal is adequate
- ➔ All **mechanized** with Coq

The Coq Proof Assistant

coq.inria.fr

CONCLUSION AND FUTURE WORK

What we did:

➔ First **fully formal** definitions of pET and pWCET

➔ **Adequacy property**: formalization of "safe IID upper bound on pET"

➔ **Prove** that our pWCET proposal is adequate

➔ All **mechanized** with Coq

The Coq Proof Assistant

coq.inria.fr

Are there **better** definitions?

- *Maybe..?*
- *Please propose your preferred definition*

  … and present an adequacy proof

CONCLUSION AND FUTURE WORK

What we did:

→ First **fully formal** definitions of pET and pWCET

→ **Adequacy property**: formalization of "safe IID upper bound on pET"

→ **Prove** that our pWCET proposal is adequate

→ All **mechanized** with Coq

The Coq Proof Assistant

coq.inria.fr

Are there **better** definitions?

- *Maybe..?*
- *Please propose your preferred definition*

  ... and present an adequacy proof

How to **derive** such axiomatic pWCET?

- *Are existing methods compatible with it?*

  (MBPTA? EVT? SPTA?)
- *Can compatibility be proven in Coq?*

CONCLUSION AND FUTURE WORK

What we did:

→ First **fully formal** definitions of pET and pWCET

→ **Adequacy property**: formalization of "safe IID upper bound on pET"

→ **Prove** that our pWCET proposal is adequate

→ All **mechanized** with Coq

The Coq Proof Assistant

coq.inria.fr

Are there **better** definitions?

- *Maybe..?*
- *Please propose your preferred definition*

  ... and present an adequacy proof

How to **derive** such axiomatic pWCET?

- *Are existing methods compatible with it? (MBPTA? EVT? SPTA?)*
- *Can compatibility be proven in Coq?*

Use axiomatic pWCET to build an **analysis**

- *We prove that any sound analysis results in valid bounds. Let's verify one!*

CONCLUSION AND FUTURE WORK

What we did:

- → First **fully formal** definitions of pET and pWCET
- → **Adequacy property**: formalization of "safe IID upper bound on pET"
- → **Prove** that our pWCET proposal is adequate
- → All **mechanized** with Coq

RTSS * Artifact * Consistent * Complete * Well Documented * Easy to Reuse * Evaluated

The Coq Proof Assistant

coq.inria.fr

Still do not like pWCET?

- *Come watch Filip's talk about **pWCET-less Correlation-Tolerant Analysis** on December 8th (Session 11 @ 12:35pm)*

Are there **better** definitions?

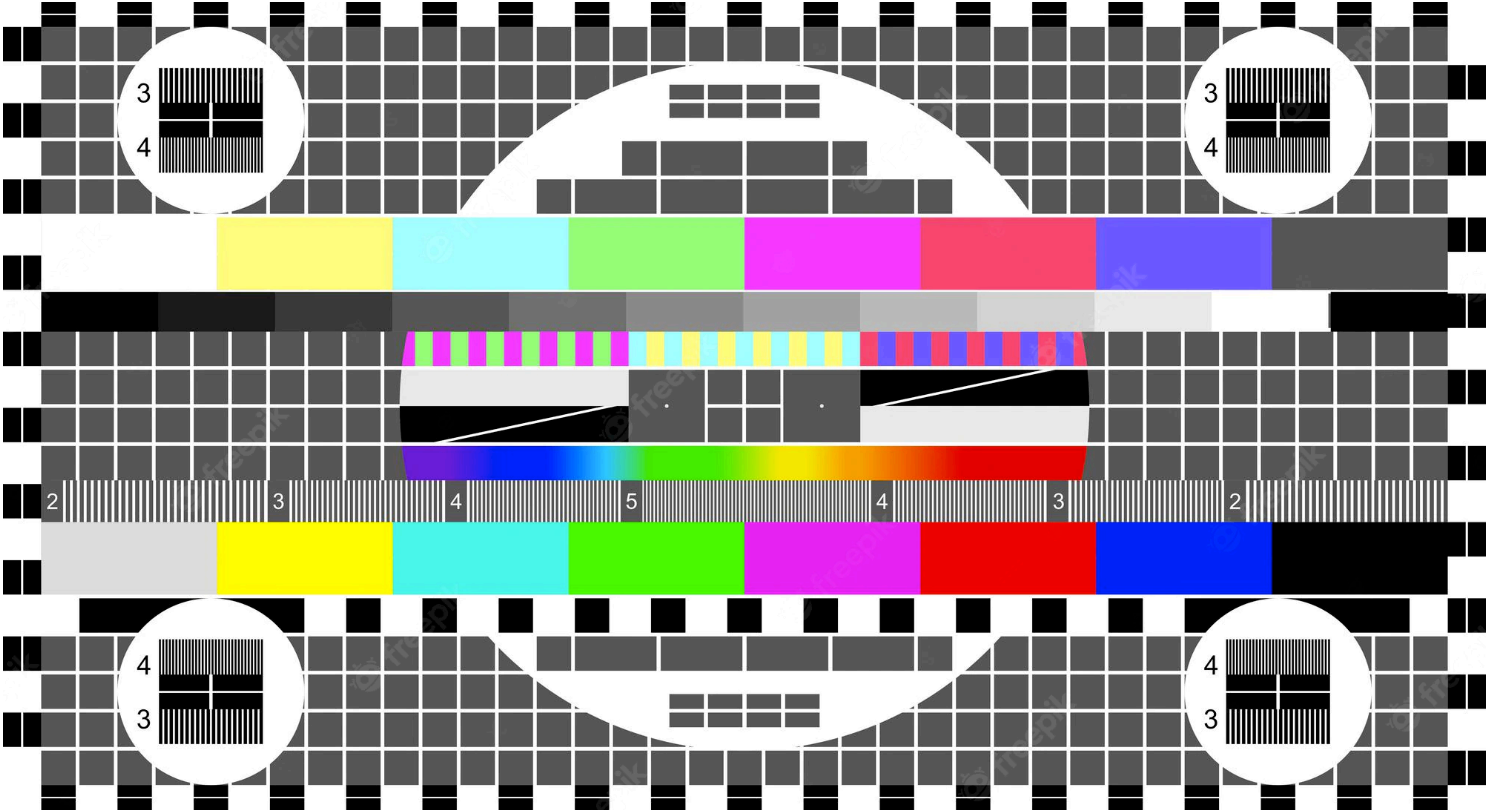
- *Maybe..?*
- *Please propose your preferred definition … and present an adequacy proof*

Use axiomatic pWCET to build an **analysis**

- *We prove that any sound analysis results in valid bounds. Let's verify one!*

How to **derive** such axiomatic pWCET?

- *Are existing methods compatible with it? (MBPTA? EVT? SPTA?)*
- *Can compatibility be proven in Coq?*


3
4
3
4
2 3 4 5 4 3 2
4
3
4
3

BACKUP SLIDES

WHY *AXIOMATIC* pWCET?

Theorem *(paraphrased)*. Consider a job $J_{i,j}$. Let $\mathscr{R}_{i,j}$ be the pRT of $J_{i,j}$ in the initial system and $\mathscr{R}^{\star}_{i,j}$ be the pRT of $J_{i,j}$ in a simplified system obtained via pWCET F_i. Then $\mathscr{R}_{i,j} \preceq \mathscr{R}^{\star}_{i,j}$.

Def. 7 (✂). *A monotonically increasing function $F_i : \mathbb{W} \to [0,1]$ with $F_i(0) = 0$ and $\lim_{t\to\infty} F_i(t) = 1$ is an axiomatic pWCET for a task τ_i if, for every $J \in \tau_i$ and every fixed arrival sequence $\xi \in \Xi$, there exists a partition $\mathfrak{S}$ (Def. 4) such that*

1) *$\mathcal{C}_J$ is partition-independent w.r.t. ξ and $\mathfrak{S}$ (Def. 5), and*
2) *F_i $\mathfrak{S}$-dominates $\mathcal{C}_J$ w.r.t. ξ (Def. 6).*

Hint:

1. Use axiomatic pWCET to construct a "copy" of the initial system, where pETs are replaced with job costs that are, **by construction**, IID and have distribution F_i
2. Prove that pRT $\mathscr{R}^{\star}_{i,j}$ in the simplified system stochastically dominates the original pRT $\mathscr{R}_{i,j}$

Weakest precondition for which we could find a proof of the adequacy property

TWO TYPES OF pWCET

Dominance pWCET [1]

- $F_i : \mathbb{W} \to [0,1]$
- Given c, $F_i(c)$ defines a bound on probability of a job of task τ_i to have cost exceeding c

If $F_i(50) = 0.999$, then out of $100{,}000$ jobs, at most 100 jobs are expected to have cost greater than 50

Confidence pWCET [2]

- $F_i : \mathbb{W} \to [0,1]$
- Given c, $F_i(c)$ defines a bound on probability that WCET of task τ_i does not exceed c

If $F_i(50) = 0.999$, no job is expected to have cost greater than 50 and we are 99.9% confident about it

[1] Davis, Robert I., et al. "Analysis of probabilistic cache related pre-emption delays."
[2] Edgar, Stewart, and Alan Burns. "Statistical analysis of WCET for scheduling."